Spring 2012

Identity management in a public IaaS Cloud

William T. Skinner III
James Madison University

Identity Management in a Public IAAS Cloud

William T. Skinner III

A thesis submitted to the Graduate Faculty of

JAMES MADISON UNIVERSITY

In

Partial Fulfillment of the Requirements

for the Degree of

Master Science

Computer Science

May 2012

Acknowledgements

I would like to extend sincere gratitude to several who have assisted in the development of this thesis. First, many thanks to my thesis advisor Dr. Florian Buchholz, whose diligent mentorship, patience and suggestions guided my research and helped me stay focused on the topics that were specifically relevant to the question at hand. I would also like to thank my other committee members, Dr. M. Hossain Heydari and Dr. John McDermott. Both of whom, provided input and guidance that helped me bring closure to this research. I especially appreciated Dr. McDermott's expertise in secure hypervisors who challenged me to the very end on the details of some of my statements. Final changes due to his reviews made this thesis much more accurate than it would have been without.

I would like to thank my wife Michelle, who bore the many nights of me being buried down in my lab working away over the last 8 months. Your support means the world to me and I look forward to sharing the success of graduation with you. Finally, I need to thank God who gave me the strength and fortitude to see this through. Without Him, I know doubt would have failed this trial.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

Abstract

In this thesis the unique environment that is the public IaaS cloud along with its differences from a traditional data center environment has been considered. The Cloud Security Alliance (CSA), states that "Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today". The CSA also points out that "there is a lack of consistent secure methods for extending identity management into the cloud and across the cloud" [1].

This thesis examines this challenge of managing identities in the cloud by developing a list of best practices for implementing identity management in the cloud. These best practices were then tested by simulated misuse cases which were tested in a prototype of the implementation strategy. The results and analysis of the misuse cases show that the implementation of the identity management solution solves the problem of managing identities for the control of the infrastructure in the cloud. However, the analysis also shows that there are still areas where the properly implemented identity management solution fails to mitigate attacks to the infrastructure. These failures in particular are attacks that are sourced from the subscriber environments in the cloud. Finally, the best practices from this thesis also present some consistent methods for extending identity management into the cloud.

1. INTRODUCTION

The subject of this thesis revolves around the study of i20dentity management in a public IaaS cloud. The term "cloud" in this thesis only refers to the underlying infrastructure, not the subscriber virtual machines. The National Institute of Standards and Technology (NIST) have published its official definition of cloud computing including what it considers essential characteristics, service models and deployment models. NIST defines Cloud Infrastructure as a Service (IaaS) as:

"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)" [2] NIST defines the Public cloud deployment model as:

"The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services" [3].

One unique quality of a public cloud is that a means needs to be provided for tenants to access and control their resources. This access occurs over the Internet which is an unsecure medium. There is a component of the public cloud referred to as the cloud control portal. This component is also commonly referred to as a self service portal. The purpose of this component is to enable users to request infrastructure and platforms as a service. This self-service portal is a gatekeeper to the automated provisioning features and other workflows provided to subscribers

by the IaaS provider. This portal is the means provided for tenants to access and control their resources.

Cloud computing environments impose new challenges on access control techniques. Existing access control techniques were originally designed for computing environments that do not share the cloud's challenges. There are four major challenges to access control methods in the cloud:

1. Multi-tenancy
2. Diversity of cloud network architectures
3. Large scale
4. Dynamic nature of cloud infrastructure

The concept of multi-tenancy is found in virtually every definition of cloud computing. A cloud can be seen as a single collection of compute and storage resources that support multiple customers or tenants. This collection can range in size and scope from a single physical server to a data center of servers. When multi-tenancy is discussed, it is assumed multiple tenants can reside on the same physical server. The primary concern of multi-tenancy in a cloud environment is the ability to isolate customer-specific traffic, data and configuration of resources using the same software and interfaces [4].

In its simplest form, multi-tenancy is an architectural model that can securely host multiple customers on the same physical infrastructure [5]. Resources are shared while providing sufficient levels of isolation to the collocated tenants. This is a simple enough definition, however with the increases in compliance and security requirements being driven by government and industry, cloud providers are required to provide more than just isolation as a prerequisite for doing business.

Today's clouds are made up of servers, storage and networking devices from multiple vendors. There can even be multiple virtualization providers used within the same cloud. There is no uniformity guaranteed within the cloud infrastructure at any level. This heterogeneous environment may have different ways of implementing access controls and managing them depending on the part of the infrastructure.

Cloud services are driving the creation of huge data centers, holding tens to hundreds of thousands of servers that concurrently support a large and dynamic number of distinct services. Amazon's EC2 Cloud contains in the neighborhood of 40,000 servers on its infrastructure [6] and their Amazon Web Services (AWS) [7] service reports over 80,000 virtual machines launched per day [8]. According to the Cisco Global Cloud Index, the number of workloads per installed traditional server will increase from 1.4 in 2010 to 2.0 in 2015. The number of workloads per installed cloud server will increase from 3.5 in 2010 to 7.8 in 2015 [9]. These statistics demonstrate the size and scale of current cloud datacenters.

IaaS clouds provide a set of interfaces for controlling virtual machines and configuring their hardware and network environment that promise a reduction in the complexity of service provisioning. However, many of these interfaces are proprietary in nature and require custom programming to integrate with the IaaS infrastructure. These customized, proprietary interfaces further complicate the infrastructure and expose additional attack surfaces of the cloud.

Access controls were not originally designed to handle such large volume and scale. In an IaaS cloud there are many systems that implement access controls in a data center. In order for these systems to be integrated into a cloud that uses an identity management system, user accounts are assigned to these systems. These user accounts are commonly referred to as service accounts. When the environment grows in complexity, more of these service accounts are required to implement the additional access controls that are present. As the number of access controls grows, the credentials that are used to manage these controls grow as well.

To reduce the work for IT administrators managing these environments, virtualization products provide several monitoring, automation, and policy-driven tools. These tools require a lot of information about various aspects of each virtual machine and other objects in the system. To support these tools and the hundreds of simultaneous users who manage the environment, the management software needs to provide secure access to the user data and information about resource objects in real-time with some degree of consistency. Such software must perform well at large-scale to accommodate the largest datacenters. [10] The need for high-performance, robust management at these scales poses challenges for these tools along with the access controls that are required to run them securely.

These challenges not only affect the methods of access controls themselves, but also the ways those methods are managed. This is especially true in an Infrastructure as a Cloud (IaaS) environment. IaaS clouds do not concern themselves with the customer virtual machines that reside on the infrastructure. In an IaaS cloud, customers are assured that the provider will not have access to their data and will not be actively monitoring their activities, save metered resource usage to charge the customer for what they use each billing cycle. The IaaS provider is then only required to protect the underlying cloud infrastructure. In the event that a security incident does occur that affects the underlying infrastructure it would be desirable that the access controls of the environment are managed in such a way that the severity and scope of such incident could be limited.

1.1 **Background and Problem Statement**

A federated identity is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. The purpose of federated identity management protocols is to simplify user management across multiple enterprise environments [11]. Single sign-on (SSO) is a subset of Federated Identity Management, in which a user's single authentication token is trusted across multiple IT systems. SSO relates only to authentication and

allows a much needed level of interoperability which is needed in the complex environment of the IaaS Cloud.

Federated Identity Management amounts to having a common set of policies, practices and protocols in place to manage the identity and trust Information of users and devices across organizations. The mapping of digital identities among different identity management realms can be difficult because a large enough set of common identifying traits needs to be matched between each of the identities for the same entity. [12]. It can be a challenge to establish that identities at different enterprises actually map to the same entity. Due to the complexity and scale of an IaaS cloud, this concept of Federated Identity Management is being considered as a strategy to manage the complex array of credentials and permissions which are used by the cloud provider and the different subscriber companies on the cloud.

The ability to share and manage identity and credentials in a seamless and secure manner is very important for being able to secure information assets in a cloud context. Having separate stores for information assets and managing them in a distributed fashion leads to many potential points of failure and also leaves a human factor open. When the human factor is introduced, a huge potential for oversights can occur which can accidentally send secure information over insecure protocols, or store them in insecure places. Many providers do not have the competency and capabilities to manage secured federated identities and credentials in a distributed and manual fashion. This is why most cloud environments rely on identity management systems which centralize and automate the management of identities and credentials. We care about Federated Identity Management because it ties to the concept of provisioning [13]. Automated bulk provisioning is of particular interest and this occurs in the IaaS cloud often.

This thesis proposes a very specific usage and configuration of directory services with Identity and access management (IAM) technologies for the management of user credentials which are applied to the multitude of access controls of an IaaS Cloud. This solution will take into account

the many attack vectors that exist against directory services in general as well as the access controls of the IaaS Cloud . The solution will be configured such that if an attack is successful, the scope of the security incident will be reduced and not lead to a large scale loss of confidentiality or data integrity to the customers whose servers are hosted in the environment. During this study, I will examine how the attack vectors of insider threats, misconfigurations and escalation attacks can be mitigated with a properly designed identity management solution. The challenges of extending a subscriber's identity management into the cloud are also considered. Currently, there are multiple protocols that subscribers use for identity management. In order to maintain trust in the cloud, a public IaaS cloud provider must also become an identity management provider to properly service its subscribers.

1.2 **Approach Overview**

As cloud computing becomes more pervasive in society and the IaaS clouds that many companies and government agencies rely on become more complex, the problem of managing the required access credentials and access controls grows increasingly more difficult. The question that needs to be answered is: will current identity management and access control methods scale with the growth of these cloud environments or will new methods altogether need to be devised to perform these critical tasks? This thesis analyzes the identity management technologies available and possible methods of configuring them to manage access controls in an IaaS cloud. The goals of the configuration methods will be to reduce the rate of configuration errors as well as the attack surface available for malicious insiders and outsiders to take advantage of for misdeeds. Then a combination of identity management and authentication technologies is proposed along with a set of best practices for implementing them. The solutions will then be compared to the current state of most implementations.

The purpose of this work is to explore identity management solutions in the cloud and to recommend a solution set of best practices that will provide higher protection from to the IaaS

cloud. Recommendations will also be made about how to best extend identity management into and out of the cloud for subscribers. The thesis doesn't cover the details of event correlation, intrusion detection, anti-malware, data loss protection or any other typically used security technologies in the cloud outside of the relationship of how proper management and auditing of credentials help secure the use of these tools.

During the background research portion of this thesis an investigation and analysis of both open source and proprietary identity management solutions occurred. However, when building the prototype of the solution and gathering metrics to measure its performance, open source solutions were primarily used. The decision to work mainly with open source solutions was supported by the following points:

- Cost was a concern since this is being prototyped in a home lab environment.
- Most of the highly detailed research available examines open standards which most open source tools are based on.
- Using open source solutions provided access to source code of the applications being used. This supported deeper examination of the technology and how it works. It also provided an additional source of data to support the validity of the proposed solution.

- The open source community provides rich support and research resources. They will be relied on heavily when examining the inner workings of how the proposed solution will operate in the IaaS cloud environment.

Any concepts demonstrated and proven with open source components should additionally translate to proprietary solutions as well because most software companies want to operate in the cloud since that is the direction technology is heading [14]. In order for proprietary solutions to work in a heterogeneous environment, these products need to implement the same open standards.

Currently, there is no universally agreed upon method for operating a public IaaS cloud. Over the next couple of years, many large environments, including portions of the U.S. governments computing environment will be moving to the cloud. This goal is specifically demonstrated by the government's new "Cloud First Policy"[15]. However, the current security posture of the cloud is such that no one trusts the platform to hold important data that needs to be kept private. The multi-tenant nature of the cloud makes many corporate executives nervous [16]. Many question the access controls and identity management present in most current IaaS clouds. [17] The cloud introduces additional threats besides the traditional external threats encountered within resident data centers. Due to the fact that the entire data center is outsourced when it resides in the cloud, the insider threat becomes amplified. This amplification is due to the reliance on the cloud administration and management staff to secure and operate the underlying infrastructure that hosts the virtual networks and servers of the tenant. IaaS provider management activities can directly affect a subscriber's virtual machines. Oversubscription of available resources can occur. Changes implemented by provider administrators have been known to impact multiple customers due to the multi-tenant nature of the cloud. This makes following a formalized, structured process for requesting, documenting, testing and implementing any infrastructure changes very important. Identity management solutions must be interwoven within all of these access controls in order to make them effective and enforceable. Rigorous auditing mechanisms must be included as well, which again are made effective by a good solid identity management solution.

This thesis shows that it is not only necessary to have a solid identity management solution, but the identity management solution be deployed in such a way that there is a distinct separation between the management of the IaaS provider and subscriber identities. In an IaaS cloud environment each should maintained on separate networks. One solution should be dedicated for subscriber activity and access rights management and the other should be dedicated

for cloud administration. At no time should a compromise of subscriber user credentials expose management credentials to possible compromise and vice versa. Due to implementation limitations a trusted arrangement needs to be in place where the subscriber identity management system trusts the provider identity management system, but that level of trust will limit access rights to a very narrow definition of maintenance tasks which will be discussed later in the thesis.

Role-based access control addresses some of the separation of duty issues mentioned above. Currently, providers rely on just role-based access control to address these issues. Most current implementations are not strict enough to create the level of trust that is required to instill confidence in larger cloud adopters. Stricter measures are required which were examined in this thesis.

The approach was to build a small scale prototype of an IaaS cloud, composed of the basic components that are discussed in the background research section of this paper: hypervisors, management interfaces, VLANS, firewalls, routers, switches, control portal, audit log aggregation, intrusion detection devices, anti-virus components, etc. The background research explains the basic functionality and usage of these subcomponents and present how these pieces are brought together in the architecture of an IaaS cloud in general. The actual prototype that was built is detailed in section 3.4.1 of this thesis. The components used for each function and why is explained, along with an architecture review which include basic data flows. Steps stand up and operate the environment are also detailed in section 3.4.1. The Background and Related Work sections present concepts about identity management systems. These concepts were applied to plan an implementation that will meet the goals of protecting the IaaS cloud from insider attacks, control portal attacks and infrastructure attacks from the customer virtual machines themselves.

In order to measure the effectiveness of the solution a series of common use cases and misuse cases were developed. The use cases came from a set of common subscriber activities and infrastructure management activities that were discovered during the background research that was performed for this thesis. Most of those subscriber activities include the provisioning and

management of the virtual machines and networking components within the resources that are assigned to them. Some of these activities are automated, such as the initial provisioning of resources to their subscriber environment. Some of the activities are manual operations such as the creation of individual virtual machines to be used by the subscriber for their designated purposes. The common infrastructure management activities may include but are not limited to, provisioning user accounts for subscriber and provider management, configuring compute and networking components in the cloud and managing security devices.

The misuse cases were derived from the background research that covers the three primary attack surfaces that this thesis is concerned (insider threats, attacks to the control portal and infrastructure compromises sourcing from subscriber virtual machines). Specific results from testing the cases in the form of audit log events were used to measure the outcomes from each use and misuse case.

For efficiency, cloud providers prefer to automate the provisioning of pre-built images of operating systems as well as other services such as databases and web services onto virtual machines. Cloud subscribers need to be sure that the IaaS provider customizes the accounts and access management on a per-subscriber basis so passwords and privileges given to one subscriber doesn't enable them to access other customer environments. This use of pre-created virtual images is one of the insider threat attack vectors. When operating systems are installed, they contain built in accounts with administrative privileges.

The top identity management challenges for IaaS providers center around the management of privileged access to virtual machines provisioned on the IaaS platform [18]. When using a pre-configured image there are a number of outcomes, which may impact operations depending upon how and by whom the image was created. Images are difficult to trust basted on meta-information such as "creator" or "owner" of the image. Both image and user authenticity should be verified securely prior to deployment.

1.3 Thesis Statement

An analysis of identity management solutions in the public IaaS cloud reveals that many issues still remain unsolved before the public IaaS cloud will be considered trusted by enterprise and government subscribers to host critical data. These unsolved issues apply to identity management solutions within the cloud itself, and those solutions that allow subscribers to extend multiple identity management solutions into the cloud.

1.4 Document Organization

This thesis is organized into five chapters. This first chapter is an introduction where background information is presented about the different challenges presented with the IaaS cloud environment when compared to the traditional private data center along with the importance of identity management within the realm of these challenges. The second chapter is an overview and analysis of the building blocks necessary to understand the IaaS cloud environment, the attack surfaces and the components of identity management solutions that exist which can be applied to the multiple components of the cloud. The third chapter presents the prototype and test approach used in this thesis. The various components of the prototype IaaS cloud which was built are detailed. The steps of the test procedures for each of the selected misuse cases are also presented. The modeling of extending identity management into the cloud from a subscriber was not able to be prototyped for this thesis, but the challenges and some recommendations of doing so are discussed in the third chapter of the thesis. The fourth chapter presents the results and analysis of the tests that were run to measure the security and effectiveness of the recommendations. Finally, the fifth chapter will present conclusions, the limitations of the thesis and discuss any related areas of future study.

2 BACKGROUND AND RELATED WORK

This chapter gives an overview of the IaaS cloud in general, including an overview of the basic conceptual architecture detailing its major components. The goals of an IaaS cloud along with its advantages and disadvantages are presented. Many of these disadvantages are linked to the difficulty of managing identities and access rights in the cloud. This chapter will also point out the similarities and differences between the cloud environment and traditional co-located data centers, because a co-located data center is the most similar environment to an IaaS cloud when speaking of traditional datacenters.

There are multiple open source and proprietary virtualization hypervisor/cloud products available today. This chapter will examine and analyze how a few of the most popular ones today handle the issues of a cloud environment. The main hypervisors that will be covered are VMware, Xen and Hyper-V. The cloud/hypervisor management products that will be covered are Vsphere, VCenter, Cloud Director, Xen Cloud Platform and Eucalyptus.

The background and related work sections will discuss the operational and security models used by all of these products along with the supported methods of identity management and access rights control available. The protocols and standards that make up identity management will be covered in this chapter as well along with proprietary and open source software products that are available to provide these solutions. Advantages and disadvantages will be discussed for each solution along with each product's possible integration points in a cloud.

2.1 Preliminaries

When an IaaS cloud is discussed, there are two major issues:

1. The cloud provider is only responsible for the security of the underlying infrastructure that they let subscribers run virtual machines on.

2. Neither the cloud provider, nor any other subscriber, even when hosted on the same hardware, should be able to view or affect the data in other subscribers' virtual machines. Also, they should not affect the operation of any objects that another subscriber is leasing and running.

There are two distinct environments in the IaaS cloud. The first environment is the cloud provider realm and the second environment is the subscriber realm. This presents a particular challenge when it comes to identity management. Ideally, no one from the provider realm should even have the capability of interacting in any way with objects in the subscriber realm. However, there is a major competing interest which is, that the provider realm has to be able to manage the components that allow the objects in the subscriber realm to operate. This competing interest can work its way around any number of access controls that may be in place. The only protection in place is the trust that is put in the cloud provider. There are different levels and kinds of trust available. The subscribers at a minimum need to have assurances that they can trust that the cloud provider will not use its administrative rights to monitor subscriber communications or interfere with operations inside a subscriber's virtual environment. These assurances need to be in the form of specific technical controls so that subscribers will have the confidence to move their data to the cloud.

Michael Armbrust states [19] that confidentiality and auditability of data leads to an extra layer of security to data. Confidentiality of data is accomplished by employing various types of encryption throughout the infrastructure. Subscribers are encouraged to use encryption at rest within the virtual machines in their environments. The IaaS provider encrypts data in transit via SSL or other VPN technologies to thwart eavesdropping on communications when the subscribers connect to their virtual machines in the cloud. The cloud provider also employs Transport Layer Security (TLS) to encrypt log file data as it is transmitted to centralized servers

that collect and correlate audit and system log data into events that inform the cloud administrators of various activities occurring on the infrastructure.

Virtualization software has been known to contain bugs that allow virtualized code to "break loose" to some extent. Incorrect network virtualization may allow user code access to sensitive portions of the provider's infrastructure, or to the resources of other users. Auditablity of these areas could be added as an additional layer of security beyond the abilities built into the applications themselves that operate on the cloud. Auditing and confidentiality are often lumped into a single logical layer. This thesis relies on auditing capabilities more than confidentiality. Cloud providers can establish more trust with potential subscribers by being more transparent about the technologies and processes that govern the virtual environment. Subscribers', internal auditing teams are required to understand the technology and processes underlying cloud computing, as well as the complex processes used to assess provider performance. Reaching out to subscribers and assisting their internal audit staff will go a long way to establish trust so that they can move to the cloud.

Identity management and auditing are specific technical controls that can provide assurance of trust to the subscribers. Auditing of administrative privileged account activity is critical to assuring trust. This audit function cannot be implemented without the presence of an identity management system. Within this thesis, auditing and logging solutions, are only discussed where they need to be when describing how identity management is involved. A deep investigation into auditing and logging systems is outside the scope of this research. Varying types of logging systems are not discussed. The inner workings of and strategies of logging and auditing are not discussed. Auditing is used in the prototype because test results which were used for analysis purposes came from system audit logs and other log sources. The remainder of this background section discusses the components of the cloud and the many methods and protocols used to provide identity management. This section also defines identity management itself.

2.2 Security of Virtualization Management Infrastructure

There are many security related aspects in a virtualized environment. One of the most basic considerations is to prevent users from interacting with each others' virtual machines. Another aspect is ensuring that a given virtual machine does not monopolize all of the computing resources on the underlying host that it resides on. This can infringe on other virtual machines and keep them from running. The management layer must block communication between customer environments that could occur due to sharing resources. Customer environments that reside on the same hardware should use virtual networking technologies to keep the separate virtual networks from communicating with one another. Finally and most directly related to this thesis, the management layer must provide roles and permissions in order to control what operations can be done by end-users vs. what operations can be done by administrators. With increasing numbers of users and virtual machines, the number of combinations of users, objects and permissions grows exponentially, and it is the responsibility of the management infrastructure to keep the overhead small while still providing sufficiently granular permissions. There are multiple virtualization platforms available, VMware, Xen, Hyper-V to name a few. Each hypervisor and supporting management applications have different architectures and methods for addressing the multi-tenancy and other security issues. It is important to understand at least the basic architecture and approaches that some of the few major hypervisors take to solve these issues before diving into the access controls that will be required and what methods are best for managing the credentials that run these access controls.

2.3 Cloud Control

From a conceptual standpoint, cloud services need some form of cloud control which enables consumers of the cloud service to manage and configure the virtual networks and machines within the environment to which they are subscribed. In IaaS based clouds the control interface allows subscribers to instantiate machines, as well as the ability to start, pause and stop

them. Machine images can be created or modified, and the links to persistent storage devices must be configured. The security of a cloud service highly depends on robust and effective security mechanisms for the cloud control interfaces. Typically, the cloud control interface can be realized either as a Simple Object Access Protocol (SOAP)-based Web Service, or as a Web application. There are other methods available, but they are outside the scope of this paper.

SOAP is n protocol specification for exchanging structured information in the implementation of web services [20] [21]. It uses XML for its message format and typically uses HTTP and SMTP to transmit its messages. SOAP can be used to form the foundation on which a web service can be built.

Many of today's applications communicate using Remote Procedure Calls (RPC) between objects, but HTTP was not designed for this. RPC traffic also carries with it many security issues so most firewalls and proxy servers block RPC traffic. A better way for applications to communicate is over HTTP, because it is not typically blocked by firewalls and it is a protocol supported by all browsers and servers. SOAP is an XML-based protocol to let applications exchange information over HTTP.

Web Services Security (WS-Security) is a flexible and feature-rich extension to SOAP to apply security to web services. The protocol defines access profiles that specify how integrity and confidentiality can be enforced on messages. These profiles also establish how messages that are involved in the federated authorization process are handled and exchanged between the clients and servers involved [22].

If the control interface is a Web application, security relies on SSL/TLS combined with some client authentication mechanisms. If the control interface is SOAP-based, then WS-Security can be applied to provide security services. For the authentication purposes, security tokens (mainly X.509 certificates) and XML Signature can be employed. A problem that generally arises is that the WS-Security standard is vulnerable to signature wrapping attacks, which consequently may invalidate this authentication mechanism. Signature wrapping attacks deceive servers into

authorizing digitally signed SOAP messages that have been changed. WS-Security is briefly discussed in the background section covering WS-Federation later in this paper. WS-Security is only one method of web services security. Some of the key topics within web services security include:

- choosing between applying security to the messages being sent and applying security to the transport mechanisms.
- choosing a client authentication technology which can be basic direct authentication or a brokered method such as x.509, Kerberos version 5 protocol or Security Token Service. [23]

There are a variety of models for authentication that can be applied when accessing a web application. A client can directly provide credentials, such as a user name and password. An alternative method would be to have a third-party broker, such as a Kerberos domain controller provides a security token for authentication. These two models are referred to as direct authentication and brokered authentication. Some web service authentication methods are compared in the background section of the thesis.

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls [24]. Username/password based client authentication may be highly vulnerable to XSS attacks, so other more secure methods should be used, such as certificates and multifactor authentication. Although as seen in the news recently, even multifactor authentication methods can be compromised. EMC/RSA suffered an attack earlier in 2011. In a letter to its customers, EMC/RSA originally stated that they had no evidence that customer security would be compromised when using RSA 2-factor authentication products [25]. Then, nearly three months

after the EMC/RSA breach, EMC/RSA announced they would replace the security tokens of nearly all of its SecurID customers. Hackers had found a way to duplicate SecureID keys that were issued to some defense contractors and breach their networks as well [26].

The cloud control component is a vulnerable component of the IaaS cloud. Web portals have a well known attack surface with many common APIs. This is why the authentication mechanisms and access controls which get applied here are crucial. Most of the issues that expose the cloud control component to possible compromise are implementation related. Passwords and shared keys are sometimes hard coded into custom components of the portal which if captured can lead to compromise. Often, there are times where competing interests may cause problems. The major interest of a developer producing code is to implement certain functionality in the portal is constrained with a dead line. At the same time, the security staff is tasked with monitoring all activities which are going on which includes this development work. The security staff slows down development, so the development staff uses its internal knowledge to circumvent security controls to get the job done on time. Application security does not exist in a vacuum and for developers; it is just one of many competing requirements that are expected to be addressed. Security controls should always be seamless and transparent [27]. Unfortunately, many security controls are not seamless, particularly to software developers. Until security controls can be made more transparent while being effective, these circumventions will continue.

Currently there is a race among cloud service providers to bring their product to market for the larger business customers. This is demonstrated by the various virtualization vendors such as VMware and Citrix, gearing most of their new products for the enterprise space [28]. Security should be a differentiating factor among these offerings, but according to many surveys it is not the top factor. The most frequently cited responses when asked about primary drivers behind moving to the cloud included: cost savings, efficiency, ease of use and flexibility [29] [30]. Eventually, it will be left up to the market to determine how important a factor that security will be. This battle will more than likely leave the cloud control portal as the cloud's weakest point.

2.4 VMware as an example virtualization platform.

The management layer designed by VMware is known as vSphere. The base vSphere architecture includes a single monitoring server called vCenter, a database for archiving configuration and performance data and agents running on each physical host called an ESXi host which runs the virtual machines. The vCenter also supports an API for third-party tools and user interface clients to perform and monitor operations on vSphere. In larger environments the vSphere layer can be enlarged to accommodate growth by using multiple vCenter servers. These vCenters do have the capability to be connected via Linked Mode [31]. Linked mode serves two main purposes. First, it allows user interface aggregation and provides a single view for the entire infrastructure. So, the user can log into a single vCenter server, and have information for all vCenters in the environment presented in that singular view. Queries for any of the ESXi servers in the environment are seamlessly redirected to the appropriate host or vCenter, no matter which vCenter in the environment that the ESXi host directly registers to. Secondly, in Linked Mode, user roles are synchronized across the vCenter monitoring servers using LDAP allowing an administrator to assign privileges once and have those privileges applied across the entire environment. This second functionality is a security concern when considering strategies for managing access control credentials in the cloud and it is an area where a lot of time will be spent.

2.5 VMware Security Model

As scale increases, the size of the attack surface increases, which makes it harder to design and administer the security policy. VMware uses several techniques to reduce the complexity. The ESXi hypervisor is responsible for isolating virtual machines from one another and making sure they don’t access each others’ state. For communication among virtual machines within and across hosts, products like vShield Zones [32] provide firewall, NAT, and intrusion

detection/prevention capabilities. In order to deal with administrator and end-user access throughout the infrastructure, vSphere provides a comprehensive permissions model. Permissions are defined as a 3-tuple, user, action, and object. This permission model is further simplified by allowing grouping in all three: users, actions and objects. A common method of implementing this model would be to create groups and assign permissions according to groups defined by the underlying user-management/authentication mechanisms (Active Directory, LDAP, etc.). Actions are grouped into roles. The system comes with a number of default roles. Customized roles are also supported. These roles, groups and settings can all be replicated to all vCenter servers grouped together in linked mode. Objects are grouped into hierarchical folders and permissions assigned at a folder level can be propagated down to any children nodes.

The default role-base access roles in ESX Servers are: Read only, Guest OS owner, VMWARE Admin and Root.

Access Right	**Default Role**			
	Read Only	**Guest OS Owner**	**VMWARE Admin**	**Root**
Access to Management UI	No	Yes - View own VMs only	Yes - all guests	Yes
Vmkusage Stats	View Only	View Only	Yes - all guests	Yes
Control Power Function	No	Yes - own VMs only	Yes - all guests	Yes
Access VMs Remotely	No	Yes - own VMs only	Yes - all guests	Yes
Access to VM configuraton file	No	Yes - own VMs only - r-x access	Yes - all guests	Yes
Create and Delete Virtual Machines	No	Yes - own VMs Only	Yes - all guests	Yes
Modify VM HardwareConfiguration	No	Yes - own VMs Only	Yes - all guests	Yes
Change Access Permissions of Guests	No	No	Yes - all guests	Yes - all guests

Service Console Access	No	No	Yes limited - use sudo for access	Yes - Full Control
Create and remove users and groups	No	No	No	Yes
Modify resource allocations for guests	No	No	No	Yes
Modify all ESX settings	No	No	No	Yes

Table 1: VMWare Default role-based access roles. [33]

These built in roles usually provide adequate functionality for the various types of users and administrators that need to operation on the cloud. If these default roles are not sufficient for an environment, then there are about 100 preconfigured privileges that can be assigned to a custom role and used. VMware's security model is very robust and includes conflict resolution for when conflicting permissions are assigned to a user account. The most restrictive permission takes precedence. For instance, if a user is part of a group in the VMware Admin role, but the user is explicitly assigned a Read-Only role on a particular object, the most restrictive permission will apply thereby allowing the user only Read-Only permissions to the object. Objects are arranged in a hierarchical order such that an object can have child objects. To ease the administrative burden of managing privileges, permissions can be enabled to propagate down to any child objects.

Virtual Center is an application that can be installed on a Windows-based operating system, or deployed as an appliance which is supplied by VMware. The appliance version runs a hardened Linux-based operating system. Virtual Center is used to manage multiple ESXi servers from a single console. Virtual Center can be installed so that it operates in a local workgroup. This configuration maps the users and groups created within the virtual center to local users and groups created on the operating system of the server. By default accounts that are local administrators on the server where Virtual Center is installed are assigned the Administrator role at the top of the inventory list in Virtual Center. Virtual Center can also be installed onto a Windows-based operating system that participates in an Active Directory Domain. Being a

member of an Active Directory Domain adds the ability to configure active directory users and groups to map to the users and groups within Virtual Center. This is the preferred configuration because it allows IaaS cloud administrators to take advantage of the identity management solution that is already in place to authenticate administrative user accounts for managing the virtual infrastructure. In this case, the only service that the identity management solution is providing is authentication. The Virtual Center is what provides authorization and accounting. By default, the Domain Admins Active Directory group will be assigned the Administrator role.

2.6 Xen as a Virtualization Platform

A computer running the Xen hypervisor contains three components:

- Xen Hypervisor
- Domain 0, the Privileged Domain (Dom0) – Privileged guest running on the hypervisor with direct hardware access and guest management responsibilities
- Multiple DomainU, Unprivileged Domain Guests (DomU) – Unprivileged guests running on the hypervisor; they have no direct access to hardware (e.g. memory, disk, etc.)[34]

The Xen hypervisor runs directly on the hardware and becomes the interface for all hardware requests such as CPU, I/O, and disk for the guest operating systems. By separating the guests from the hardware, the Xen hypervisor is able to run multiple operating systems securely and independently. Domain 0, a modified Linux kernel, is a unique virtual machine running on the Xen hypervisor that has special rights to access physical I/O resources as well as interact with the other virtual machines. All Xen virtualization environments require Domain 0 to be running before any other virtual machines can be started. A system administrator can log into Domain 0 and manage the entire computer system. Guest virtual machines are either run with a special modified operating system referred to as paravirtualizion or un-modified operating systems leveraging special virtualization hardware (Intel VT and AMD-V) referred to as hardware virtual

machine (HVM). Note – Microsoft Windows requires a HVM Guest environment [35]. All paravirtualized virtual machines running on a Xen hypervisor are referred to as Domain U PV Guests [36]. These guests are controlled by the Domain 0 and independently operate on the system. Domain U guests are referred to as unprivileged and have no direct access to physical hardware on the machine as the Domain 0 guest does. Domain U PV Guests are modified Linux operating systems. Other Domain U PV Guests can be Solaris, FreeBSD and other UNIX operating systems. The Domain U guest virtual machine knows that it does not have direct access to the hardware and recognizes that the hardware contains other virtual guests. Xen uses a daemon called Xend which is a python application to be the system manager for the Xen environment. XML RPC is used to send all requests to Xend. There is a Xenstored daemon that maintains a registry of information between Domain 0 and all other domain U guests. The Domain 0 virtual machine uses this registry to setup device channels to the other virtual machines. The Xen Hypervisor is operating system neutral [37]. Due to this independence Xen is capable of letting many different types of Linux based operating systems be the Domain 0. This allows more flexibility in Xen deployments.

2.7 Xen Cloud Platform

The Xen Cloud Platform (XCP) is an open source enterprise-ready server virtualization and cloud computing platform, delivering the Xen Hypervisor with support for a range of guest operating systems including Windows and Linux network and storage support, management tools in a single, tested installable image, which is also called XCP appliance.

XCP addresses the needs of cloud providers, hosting services and data centers by combining the isolation and multi-tenancy capabilities of the Xen hypervisor with enhanced security, storage and network virtualization technologies to offer a rich set of virtual infrastructure cloud services. The platform also addresses user requirements for security, availability, performance and isolation across both private and public clouds [38].

2.8 Eucalyptus Open Source Platform and User Identity

Eucalyptus enables the creation of on-premise private clouds, with no requirements for redesigning the organization's existing IT infrastructure or need to introduce specialized hardware. Eucalyptus implements an IaaS private cloud that is accessible via an API compatible with Amazon EC2 and Amazon S3 [39]. Eucalyptus user identity management can be integrated with existing Microsoft Active Directory or LDAP systems to have fine-grained role based access control over cloud resources [40].

The need for private cloud environments fostered the development of freely available open source implementations of the cloud systems. Among other advancements, the Eucalyptus cloud implementation [41] gained a lot of public attention and was integrated into the well-known Ubuntu operating system (Ubuntu Server Edition). As of today, Eucalyptus is of the world's most widely deployed software platform for IaaS clouds with more than 25,000 deployments to date [42]. As far as functionality is concerned, the cloud management interfaces of Eucalyptus were designed to copy the Amazon cloud control interface in order to support a switch from the prominent pre-existent Amazon EC2 cloud to a Eucalyptus cloud. Nevertheless, it must be stressed that the functionality and security mechanisms have been implemented independently. Every Eucalyptus installation by default provides almost the exact same interfaces as the Amazon EC2 cloud. It should also be noted that the Eucalyptus SOAP interface provides the same methods as the Amazon EC2 interface. It also puts forth a customized Web front-end for a manual cloud administration. Finally, being hypervisor agnostic, Eucalyptus can be used to manage a cloud using any virtualization technology.

2.9 Access Control Implemented in Modern Operating Systems

Access control is usually defined as a relational model over the following domains: the set of subjects S, the set of objects O and the set of rights R [43]. Modern operating systems make

access-control decisions using configuration metadata such as access tokens and access-control lists. This metadata is stored in multiple formats which can be manipulated in various ways to influence what is seen as access control behavior. In operating systems, the access-control model is typically implemented with a reference monitor using a data structure called the access matrix. The access matrix can be stored one of two ways. First, it could be stored as an access list, which is associated with a resource (object) and is the list of all principals (subjects) and their permissions on the given resource. Secondly, it could be stored as a capability list which is the list of resources and associated permissions a given principal is capable of accessing. Most access-control models also impose further restrictions or constraints. An example of an additional constraint is that most access-control models include the concept of ownership.

When discussing access control methodologies, there is usually a debate concerning white listing vs. black listing. Both strategies have their place and it is helpful to recall what works where. A blacklist or block list is a basic access control mechanism that allows everyone access, except for the members of the black list. The opposite approach is a white list, which denies everyone by default and only allows the members of the white list [44]. Firewalls generally work on a white list model: if you are an approved protocol, you are allowed into the network, otherwise the traffic is blocked. An e-mail spam filter may keep a blacklist of addresses, any mail from which would be prevented from reaching its intended destination.

Traditionally, execution control has been based on a blacklist. Computers are so complex and applications so varied that it just doesn't make sense to limit users to a specific set of applications. The exception is constrained environments, such as computers in hotel lobbies and airline club lounges. On those, you're often limited to an Internet browser and a few common business applications. Lately, we're seeing more white-listing on closed computing platforms [45]. For example, if you want a program on your smart phone (Android, iPhone, etc.) you need to have that program approved by the phone manufacturer and included in their online store so that it can be deployed to the phones. This is most likely being done because the smart phone

developers want to control the economic environment, but this feature is still being sold as a security measure.

It is important to understand the complexity involved with how operating systems, whether it is the hypervisor, the system that the management platforms for the hypervisors run, or the guest operating systems themselves implement the concept of access control. This complexity is ignored in many cloud environments and becomes the source of many misconfigurations.

User accounts can be placed into groups for easier application of rights or permissions to those user accounts. However, these groupings become more complicated due to the fact that a user account can typically be a member of multiple groups. The nesting of groups can continue to add to the complexity. An administrator may find that a user account may have more or less access rights than they expected. This can occur on occasions where a user account is not directly assigned rights to a resource, but a group that the user account belongs to is a member of a group that has rights to that resource. Due to the way an operating system computes the access token of the user account, a user account's access right to a resource may differ depending on whether the object is accessed over the network or locally. This situation is compounded when conquering these hurdles in a cloud environment. Even the most experienced system administrator has a huge task in trying to document and understand the full nature of an IaaS Cloud's user account environment. That is why the research of account management and access controls in an IaaS cloud are so important. The government and many pivotal businesses in this country are moving full speed ahead to move their information infrastructure to the cloud in order to save countless hundreds of thousands of dollars [46]. If something as basic as configuration best practices is not understood, then these large scale cloud deployments will remain highly vulnerable and the trend of high profile attacks from 2011 will continue to multiply.

2.10 Identity and access management (IAM)

Identity and access management (IAM) is a system of systems, techniques and processes to ensure the proper establishment and control of identities, the assignment of privileges to those identities, and then controlling access based on those privileges [47]. Most organizations that are planning on utilizing cloud computing services need to ensure those mechanisms are appropriately integrated into their cloud plans. When identity management is brought into the cloud there are multiple identity domains to consider, each with many questions and decisions that need to be made. The two major domains to consider are the administrative domain and the customer domain. Most of this thesis is geared towards analyzing the administrative scope of IAM in the cloud. The customer scope is equally important and complex.

Two of the most important questions to consider when a company moves to the cloud are:

- What type of identity validation is acceptable?
- Will outside Identity stores be trusted or just local stores?

There are two primary mechanisms by which identities are validated. The first is organizational validation where the identity of a person is confirmed by the organization that is creating the identity. The second is personal, where someone is validated simply on the fact that they say who they are. Typically, there is a moderate amount of trust associated with organizational validation and a much lower level of trust associated with personal validation. Organizational validation is typically the method that is employed by businesses and personal validation is typically used when individual consumers are validating their identity.

The next question that needs to be addressed is what sources of identity will be accepted by the cloud subscribers and cloud provider. Policies, contracts and regulations will govern if the identities that others have asserted can be used. These issues will have a fundamental impact on how an identity management solution gets implemented. If the customer or provider requires that

identities be formally vetted in house, they will align themselves with federated identities. If vetting is not required they can rely on a simple local identity store. The advantage of federated identities is leveraging the identity management aspects of the different organizations that are part of a federation. The disadvantage of federated identities is that trust in other organizations is required. The trade-off between federated and local is ease of management versus trust.

Companies should utilize organizational-based assertions for business-related purposes, but for consumer-focused services, self-assertion may be an acceptable option. The next question that needs to be answered is what sources of identity are acceptable? Do an organization's policies, contracts or regulations, allow identities that others have asserted? Are all identities required to be vetted? The answer to these questions will have a fundamental impact on how a company can proceed. The former is typically associated with federated identities, whereas the latter is a local identity store. When discussing federated identities, there are two prevalent standards are in use: Security Assertion Markup Language (SAML) and WS-Federation. The advantage of federated identities is leveraging the identity management aspects of the different organizations that are part of a federation.

One of the issues with trust is that it is dependent on how those other organizations actually assert identities, or validate the identities of their users. Think of organizational assertion as utilizing your corporate identities to authenticate to a partner. The partner is relying on the fact that your organization has vetted you and is assigned you an ID and accepts your organization's assertion of who you are. It's important to note that in order to enable this type of identity assertion, your enterprise IAM will need to be extended into the cloud. Extending an organization's identity services into the cloud is a prerequisite for strategic use of on-demand computing services. Given this prerequisite, IaaS cloud providers must provide a robust, easy to manage, secure IAM integration to customers. This is one of the primary issues that must be solved in order for a cloud provider to be successful.

2.11 Federated Identity Management

Centralized identity management solutions, such as Active Directory or Novell Identity Manager were created to help deal with user and data security where the user and the systems they accessed were within the same network, or at least the same security context. Today, users are accessing external systems which are outside of the typical centralized domain where their user account exists. Also, there are external users who need to access internal systems. Both of these situations are typically the case with an IaaS Cloud. There are external users who will be managing virtual machines on the network. They also need to be able to make network changes without affecting other customers that may or may not be using the same hardware platform. There is also a separate management network that the IaaS provider must control access to and this network is very large and complex. The management network contains a multitude of heterogeneous devices that don't natively all communicate with any one centralized identity management solution.

This decentralization of user credentials has been brought about by the integration of business processes and everyday life into the Internet. With cloud computing taking advantage of some of these same exact technologies that have made the Internet so critical; it is only natural that the cloud shares some of these same identity management issues. Evolving identity management challenges, and especially the challenges associated with cross-company, cross-domain issues, has generated a new approach of identity management, known now as federated identity management.

The "federation" of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. It can also be used to restrict and limit access to those domains as

well. Both of these points become equally important in the multi-tenant environment of an IaaS cloud. [48]

Federation is enabled through the use of open industry standards and/or openly published specifications, such that multiple parties can achieve interoperability for common use cases. Typical use-cases involve activities such as cross-domain, web-based single sign-on, cross-domain user account provisioning, cross-domain entitlement management and cross-domain user attribute exchange. In the cloud it usually includes creating user accounts for customers in a management domain and allowing those users granular access to a logical container that will contain the virtualized environment that they are leasing from the IaaS provider.

This federation can increase security and lower risk by enabling the IaaS provider to identify and authenticate a user once, and then use that identity information across multiple systems if need be. Federation helps administrators centralize creation of user names and passwords, and specify roles and access levels for IT resources across the cloud. This greatly simplifies the task of administrators, as they save the effort of managing administration for multiple systems separately for each other.

This is very important when authenticating the administrative access users who manage the cloud. These users need to have full access to manage all of the different infrastructure equipment and software that the IaaS cloud runs on while not having any rights or management to the virtual machines that are being run within the customer environment. Federation also improves privacy compliance by allowing the user to control what information is shared, or by limiting the amount of information shared.

Organizations for the most part have not yet adopted an all in the cloud strategy. However, they have begun adopting a hybrid approach, where organizations are targeting non mission critical applications and easy to move applications such as email and collaborative portal sites such as Share Point. These hybrid solutions require identity federation in order to provide single sign on but also to maintain role based access controls between an organization’s internal

services that reside onsite and external sources that reside on the IaaS cloud. IaaS cloud providers need to support the extension of directory services such as Microsoft Active Directory into the cloud while not interfering with their own directory services that is used to manage the infrastructure of the cloud. To support this, trust must be established between the subscriber's network and the cloud so that identity information can be exchanged.

Although many organizations may understand what identity federation is, some still find it hard to see where it fits with their current environment. When identity federation is examined further, it is nothing more than user's information that is stored across multiple identity management systems and linked to a single entity. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain easily and without redundant user administration. The goal requires all included systems to use the same protocol for maximum interoperability. The notion of identity federation is extremely broad, and also evolving. It can involve high-trust, high-security scenarios as well as low-trust, low security scenarios. The term "identity federation" is by design a generic term, and is not bound to any one specific protocol, technology, implementation or company. One thing that is consistent, however, is the fact that "federation" describes methods of identity portability which are achieved in an open, often standards-based manner [49].

There are technical and organizational challenges to cloud federation. The cloud industry must establish a common authentication scheme. Cloud providers also need a way to assure data and application security and secure connectivity between clouds. Finally, cloud federation requires a billing and reconciliation system that can properly bill and compensate participating cloud service providers. Individual cloud providers can work out some of these cloud federation management challenges on a case-by-case basis, but this will require a lot of work on the part of service providers, vendors and partners.

2.12 Role-Based Access Control (RBAC) In the Cloud

One of the most challenging problems in managing large networks is the complexity of security administration. “Role-Based Access Control (RBAC) is a nondiscretionary access control mechanism which allows and promotes the central administration of an organizational specific security policy” [50]. Ferraiolo states in his original formal definition of RBAC that a role specifies a set of transactions that a user or set of users can perform within the context of an organization. Access control decisions are often based on roles and responsibilities that are assigned to a specific job function within an organization. RBAC introduces roles as an abstraction between users and privileges. RBAC never directly assigns privileges to users [51].

There are two core principles of access control that are paramount to maintain in the cloud environment. They are the principle of least privilege and separation of duties. The principle of least privilege says that a user only be given the privilege needed to perform their assigned job. In order to enforce the principle of least privilege the user’s job must be identified and the minimum set of privileges required to perform that job must be determined. A white list approach should be used to assign these privileges to a user while denying every other available privilege. By denying to users transactions that are not needed for their job, those denied transactions or privileges cannot be used to circumvent security policy established by the organization. Separation of duty requires that for a particular group of tasks, no one person is allowed to perform all of those tasks. Separation of duties’ primary goal is to deter fraud. Fraud typically occurs if an opportunity exists for collaboration between related job functions. By properly separating related duties, such as approving of expenses and paying them out, instances of fraud can be greatly reduced.

RBAC mechanisms can be used by system administrators to centrally enforce policies of least privilege and separation of duties. RBAC, teamed with a solid implementation of an identity management solution can ease the implementation of these two core principles in an IaaS Cloud. Background research into the many different commercial and open source hypervisors available

shows that the management tools included with them all use some implementation of RBAC to manage access and permissions to the virtualized environment. As of 2010, the majority of users in enterprises of 500 or more are now using RBAC, according to the Research Triangle Institute [52].

Cloud software vendors such as VMware and Eucalyptus are basing their security administration models on RBAC. You can configure VMware vSphere so that identified users can perform only a specific and focused function. Following the RBAC model, roles for particular job functions can be created within vSphere and each role can be given the subset of permissions or privileges needed to perform that function and no more [53].

Due to the scale of an IaaS cloud, there is no other current model that could easily manage the security administration of more than 500 users, much less the security administration of multiple enterprises of more than 500 users. There are many other virtualization management tools being produced by third party vendors, vKernel, NetApp and Solarwinds, to name a few. These tools are not always completely integrated into the roles and permissions built into the underlying hypervisor management servers such as VMware's vCenter, Citrix's XenConsole or Microsoft's System Center. These tools typically are given administrative rights to perform tools like cloning virtual machines and editing configurations of various virtualized resources. These elevated rights are granted to the tools outside of the RBAC configuration via local access rights to the virtual environment. When using these third party tools for management, an organization can unwittingly allow administrators to circumvent their security policies. When these tools are not properly implemented, administrators can take advantage of the tools' elevated access rights to escalate their own privileges. This demonstrates the importance of centralizing the RBAC implementation in a cloud. Without a centralized implementation, RBAC can lose a lot of its power in the cloud.

The security management tools all use service accounts to access the virtual environment details to gather data. This is a standard configuration for any application that requires privileges

in a computing environment. Each of these tools uses a directory service such as LDAP just for authentication, not for authorization. When a user operates one of these third party tools, they can gain the elevated rights that have been assigned to the tool's service account. So, since the security management tool's service account must have at a minimum read-only access to the entire virtual environment, a user who is restricted to just one set of virtual machines could login to these management tools and see all of the virtual machines, networks, storage devices and other resources in the environment. Due to this possibility of data leakage, these security management tools lack basic multi-tenant capabilities and until their centralized RBAC implementation is tightened, should be avoided in the IaaS multi-tenant environment.

Security management tools also offer the ability to perform tasks on a user's behalf through their user interface. However, they do this using a delegate user. Because they have used a delegate user, there is now an audit trail correlation issue. The issue is that only the delegate user account name appears in the audit logs. The actual users accounts operating the tool may not be correlated to the actions performed with the tool. While this correlation issue already existed within VMware vCenter and other management tools, it gets worse when you add yet another delegate user. You can audit data within vCenter but can't follow who did what, when, where, or how on the host (hypervisor). The only recourse on a host is currently to correlate the log files between vCenter and the host and if the time servers are not syncronized this correlation is impossible. You can audit all actions within the vSphere Client but once a delegate user is in use within vCenter, the audit trail breaks down to the host, and you once more need to correlate timestamps within log files to determine who did what when where and how. There are Security Information and Event Management (SIEM) solutions such as RSA Envision, Nitro Security and Splunk which can do this for you. But it would be easier if this correlation issue could be resolved within the virtualization management tools themselves. Unfortunately, there is no interface from hypervisor vendors or a third party that offers this functionality yet.

2.13 Attack Surfaces on the IaaS Cloud

The configuration of an IaaS cloud can be very complex. When configuration errors are made, internal and private information can be inadvertently exposed to everyone on the Internet. Tools are being developed to exploit misconfigured cloud services. One example is a tool that has been created to exploit the Amazon S3 misconfigurations.

Amazon Simple Storage Service (S3) is probably one of the most popular cloud services in use today [54]; it's used by major websites, corporations, governments and even private individuals. Amazon S3 is popular [55] because it's easy to link into existing applications, as all storage is presented through standard Web (HTTP) calls. A website could easily reference the Amazon S3 storage to pull over images or code to save on bandwidth and storage costs, for example. Each Amazon S3 instance is referred to as a bucket. There is a configuration option of marking each bucket as either public or private depending on usage. Each Amazon S3 customer is also required to have an account name that is unique across all of the S3 buckets around the world. This allows customers to easily access their specific bucket with a custom URL, such as http://s3.amazonaws.com/accountname. A security researcher observed the following when considering how Amazon S3 storage functioned: If each URL was customized with a unique account name, it would be possible to use existing brute force techniques to enumerate the Amazon S3 buckets and possibly access the files. He developed a tool to test this theory using standard wordlists and running them against the Amazon S3 API. The tool can also test whether the Amazon S3 storage bucket has been properly configured for public or private access. [56]

A test was run that revealed a large amount of publicly accessible buckets. Customers may not have configured the storage properly for public/private access and inadvertently exposed private data to the Internet. There were a large number of pictures stored in the Amazon S3 storage buckets and many are personal in nature, i.e., pictures of children, vacations and special events. However, there were also customer invoices and sensitive documents containing Social Security numbers and other private data that probably was not meant to be shared [56].

Multi-tenancy in virtual machine based cloud infrastructures with the way physical resources are shared between guest virtual machines produce new sources of threat when compared to the traditional data center. Malicious code may escape the confines of its virtual machine and interfere with the hypervisor or other virtual machines on the same host. There is a group of Metasploit modules called "Virtualization ASsessment Toolkit" (VASTO). VASTO's collection of Metasploit modules is meant to be used as a testing tool to perform penetration tests or security audit of virtualization solutions [57]. These attack modules can break through the virtual machine and gather information about the underlying hypervisor. These attack modules take advantage of vulnerable un-patched hypervisors and exploit existing vulnerabilities to perform their attacks. They can also be used to copy other guest virtual machine images so that an attacker could mount them locally and obtain the information in them.

Downloading and examining the VASTO package reveals that the attack plugin responsible for stealing other guest virtual machines is called "vmware_guest_stealer.rb" [58] The following description is included in the code:

```
'Name'        => 'VMware Guest Stealer',
 'Version'     => '0.2',
'Description' => 'This module exploits vulnerability CVE-2009-3733,
                  reimplementing the guest stealer exploit by Morehouse &
                  Flick. Change the port to 443 to get into an ESX server.   Works
                   on Linux hosts.
```

CVE-2009-3733 [59] warns of a mishandled exception on page faults. An improper setting of the exception code on page faults may allow for local privilege escalation on the guest operating system [60]. Reviewing the code of the module reveals that the code calls other Metasploit exploit payloads to open an SSL connection to the target ESXi host on port 443. Then, via a raw request, the attack code sends the URI '/etc/vmware/hostd/vmInventory.xml' with a get request to obtain the vmInventory.xml file and enumerate the datastores of the ESXi host. With the virtual hosts contained in the datastores enumerated, the attacker can pick a virtual host to download. Once one is chosen, a URI is crafted that traverses the data store to the location of the

virtual guest's vdmk file, which is its virtual hard disk. Then the exploit downloads the virtual hard drive to the attacker. Once the Metasploit module was able to exploit the vulnerability described in CVE-2009-3733, the steps described in the vmware_guest_stealer.rb module are pretty elementary.

Most hypervisors have the ability to move a virtual machine image from one host to another while not actually powering down the virtual machine. These activities are called live migrations. The additional software and configuration steps to allow live migrations provide the potential for additional attacks. A group of researchers at the University of Michigan published a proof-of-concept called Xensploit which allows an attacker to view or manipulate a virtual machine during a live migration [61]. Xensploit was shown to work with both Xen's and VMware's version of live migrations. There are three classes of threats against live migrations: Control Plane, Data Plane and Migration Module. The control plane employs communication mechanisms to initiate and manage live migrations. It is important that these communication mechanisms are authenticated and resistant to tampering. This is one of the areas where identity management becomes important. During a live migration, the information that is currently in a virtual machine's memory is passed, unencrypted across the network. The data plane and migration module must also be secured and protected against snooping or tampering with this unencrypted data.

The security of live migrations is still a new area of research The vulnerability demonstrated by Xensploit has not been seen in the wild; however it is a reminder that cloud administrators need to assure that the network used for live migrations is secure. On an insecure network, man-in-the-middle attacks can target both virtual and physical machines. The techniques published are novel in that they target the contents of migrating virtual machine memory to capture credentials and data, rather than going after similar information flowing across internal network transactions. Encryption of all data in transit is a much used mitigation for these man-in-

the-middle attacks. However, a majority of the data that flows through the cloud network is unencrypted. This indicates that other adequate mitigations exist. Many host hardening best practices are used as well as network isolation. Typically, migration traffic is protected by isolating the local area network that the traffic travels on.

Another attack vector is the mapping of a cloud infrastructure. Researchers have demonstrated an approach with an IaaS by launching multiple virtual machine instances from multiple cloud subscriber accounts and using network probes, assigned IP addresses and domain names were analyzed to identify service location patterns. Building on that information and general technique, the plausible location of a specific target virtual machine could be identified and new virtual machines instantiated to be eventually co-resident with the target [62]. Once a target is location is discovered, a virtual machine could be placed and tools used to break out of the hypervisor and perform tasks that could affect the performance of or possibly monitor leaking information from the target virtual machine.

3 PROTOTYPE AND TEST APPROACH

This thesis explores the importance of identity management in a public IaaS Cloud. In this paper, identity management has been examined from two major perspectives. One perspective is examining what mechanisms and strategies are available to extend a cloud subscriber's already existing IDM infrastructure into the cloud, so that they can leverage their existing identity data and continue trusting their identities in the cloud. Another perspective, one which this thesis is more specifically concerned with is how an IaaS cloud provider should configure its own IDM infrastructure to best mitigate risks against the IaaS infrastructure itself and the subscribers virtual infrastructures.

A goal of this thesis is to develop a strategy for deploying an IDM solution in the cloud to mitigate risks and demonstrate the solution for analysis. In order to do this, a prototype IaaS cloud was built in a lab. There are many components not in the prototype that are usually included in a true IaaS commercial cloud. Due to budget and scope, some components were omitted that could be considered critical by others and the thesis will try to capture the details of these components as observed in other environments during the analysis when required. The main purpose of this prototype is to observe the operation of particular cloud components when interacting with the proposed implementation of an identity management solution. A few misuse cases will be tested in this environment so that quantifiable data, in the form of audit log events from various devices, can be collected and used as results from the tests. These results were analyzed and discussed in order to show the benefits and short comings of the proposed implementation.

These ten points are the top considerations for implementing Identity management in the cloud, more especially, implementing Active Directory in the cloud:

1. The time settings of all components in the IaaS Cloud must be synchronized to the same time source and should be set to GMT time, no matter what time zone the equipment is located in.
2. The RBAC security model should be used for user account administration and management of access rights.
3. To provide additional security and to clearly distinguish between subscriber zone and management zone, the customer user objects are segregated into a dedicated subscriber domain as pictured below.

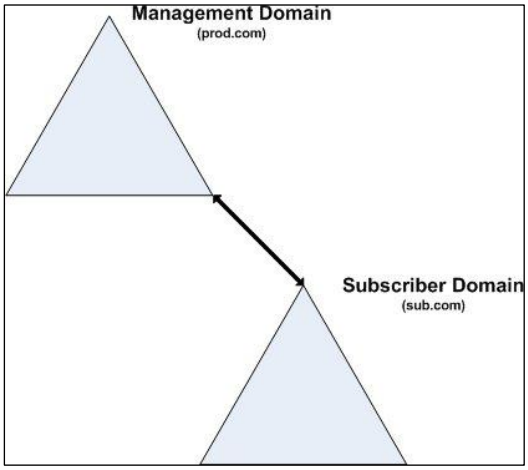

Figure 1: Identity Management Domain Structure

Accounts for all tenants are located within the subscriber's domain. It is best practice to implement a dedicated Organizational Unit (OU) within the subscriber's domain for each tenant and use groups to implement RBAC.

4. The domain infrastructure providing the adminstrator user credentials should reside within the IaaS Cloud on different networks than the subscribers virtual networks. (Out of Band Network)
5. Active Directory Trusts are required to be set up such that the subscriber and provider trusted one another. Configuration attempts of a one way trust where the provider only

trusted the subscriber failed to support all configuration needs. The subscriber needs to create and administer user accounts and groups in the subscriber domain. Additionally, VMware authentication did not work properly in the prototype when a one-way trust was in place. VMware also has other issues with its Likewise component currently. Likewise is the component that VMware uses to authenticate to an Active Directory forest. These issues will be described later along with the workarounds.

6. To implement this two domain Active Directory model, all of the VMware hosts were joined to the provider domain, and then Active Directory group nesting was employed to allow subscriber user accounts to operate on their virtualized environments on the VMware hosts. A domain local group was created in the provider domain that was assigned appropriate permissions to the VMware hosts. Universal security groups were created in the subscriber domain that contained the user accounts that were administrators within virtualized containers on the VMware hosts. Within Active Directory, Universal security groups have the property that allows them to be nested into the group of another Active Directory domain when a trust exists between the two domains [63]. The Universal groups from the subscriber domain must be nested in the proper domain local groups in the provider domain that have the permissions to the VMware hosts. Then, the permissions within VMware were mapped to the proper domain local groups that contain the nested subscriber groups.

   In the prototype environment ESXi is used for the hypervisor. When the prototype for this thesis was built implementation issues that the current version of ESXi has with its Active Directory integration were discovered. These implementation issues forced the prototype integration with Active Directory to be implemented in a different manner than what is recommended in the thesis. The details of the Active Directory implementation

issues along with the work around used and future solutions will be discussed in section 4.1 of this paper.

7. Due to the provider's use of pre-built virtual machines and automated deployment mechanisms to subscribers, unique virtual machine administrator account passwords are a concern. A mechanism must exist to customize pre-built virtual machines when they are automatically deployed to subscribers. Most guest operations systems have APIs available to allow this. The provider should include calls to these APIs in their automated deployment scripts to make this customization.
8. Centralized logging and auditing of all system and user activity is essential.
9. Subscribers should be able to extend their own identity management solution into the cloud. To support this, a site to site VPN tunnel should be extended from the subscriber's virtual container in the cloud to their premises where the rest of the subscriber's network resides. In the case of extending the subscriber's Active Directory domain into the cloud, a domain controller should reside in the cloud in addition to any domain controllers that the subscriber has on their network.
10. A separate, on demand administrative VPN connection should be available to the subscribers in order to manage their virtual machines and networks on the cloud. A SSL VPN is very useful for this purpose.

These ten recommendations cover the most common concerns discovered during the background research phase of this thesis. They outline strategies and mechanics of implementing identity management in an IaaS cloud. These recommendations also take into account personal observations made while employed as an information security engineer at an IaaS cloud data center. The recommendations regarding implementation of a centralized logging solution are a direct result of the challenges faced when configuring a logging solution in an IaaS cloud. Much of the background research for this thesis stressed the importance that extending identity

management into the cloud from a subscriber's network contributes to the trust in a cloud. This concern, led to the inclusion of basic guidelines for extending identity management into the cloud as part of the recommendations.

3.1 Approach Components and Details

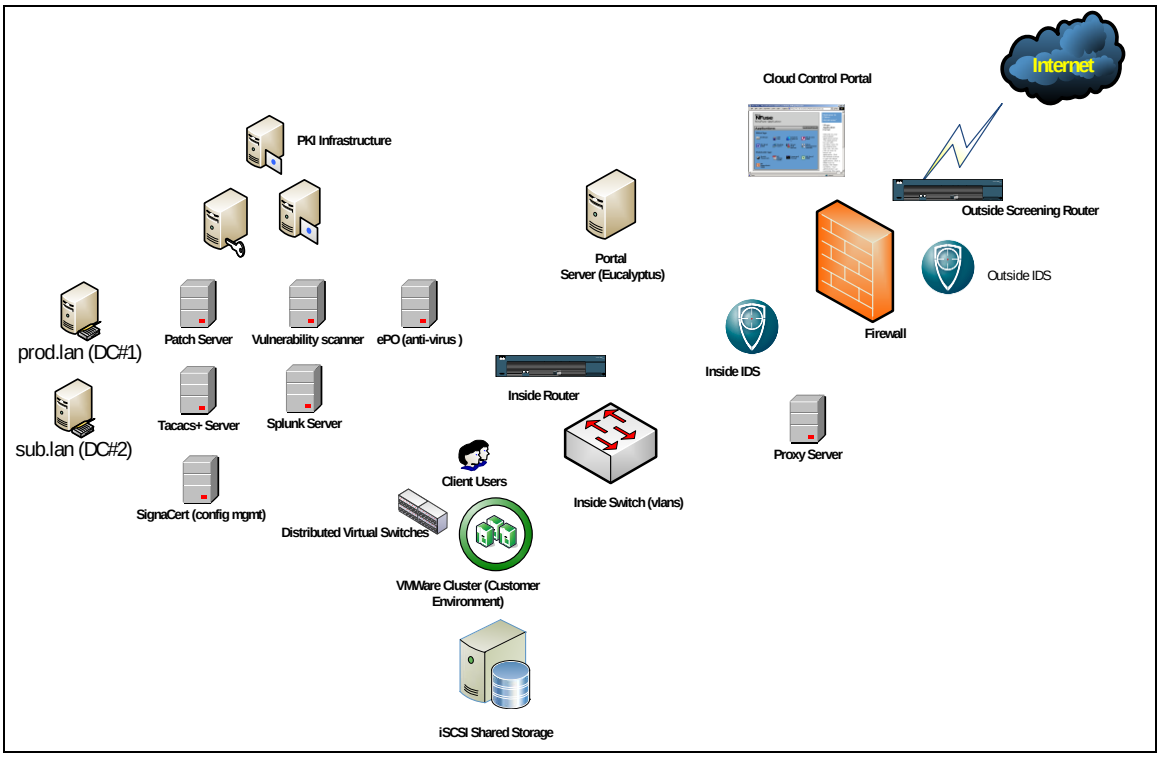

Figure 2: Logical Overview of Prototype Environment

This overview shows that the prototype cloud is made up of about twenty different intermingled and dependent services. In the lab, this mapped out to about thirty different physical devices. The details of the various services are described below. The most important part of the implementation that should be pointed out is that there are separate user databases for the subscriber user accounts and the provider user accounts. Microsoft Active Directory was used for the identity management solution, so this required two separate Active Directory Domains with an Active Directory trust relationship between the two. The domain designated for the subscriber user accounts trusts the forest designated for the provider's administrative user accounts. The

following sections 3.1.1 – 3.15 will list and detail the specific components in the prototype environment.

3.1.1 VMware Cluster

vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts. Within a vSphere HA cluster, a single host is the master host to communicate with vCenter Server and to monitor the state of the other, slave, hosts and their virtual machines. Different types of host failures are possible, and the master host must detect and appropriately deal with the failure. The master host must distinguish between a failed host and one that is in a network partition or that has become network isolated. The master host uses data-store heart-beating to determine the type of failure.

In most IaaS clouds there would be many more of these VMware clusters and they would be made up of many more ESXi hosts. This prototype will contain a single 2-node VMware cluster in order to simulate most of the functionality that would be available for a customer to use. This will help create a minimal environment that allows demonstration of the use cases that are developed for this research.

3.1.2 Distributed Virtual Switches

A distributed virtual switch acts as a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across hosts. Like a vSphere standard switch, each vSphere distributed switch is a network hub that virtual machines can use. A distributed switch can forward traffic internally between virtual machines or link to an external network by connecting to physical Ethernet adapters, also known

as uplink adapters.

Distributed virtual networking configuration consists of three parts. The first part takes place at the datacenter level, where virtual distributed switches are created and hosts and distributed virtual port groups are added to the switches. A distributed virtual port group is a port group associated with a distributed virtual switch and specifies port configuration options for each member port. Distributed virtual port groups define how a connection is made through the distributed virtual switch to the network. The second part takes place at the host level, where host ports and networking services are associated with the virtual network distributed switches either through individual host networking configuration or using host profiles. The third part takes place at the virtual machine level, where virtual machine NICs are connected to distributed virtual port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the virtual network distributed switch itself [64].

One major observation about virtual networking in the VMware environment is that extreme caution should be taken with network interfaces and virtual switches that are connected to the management network in the virtual environment. Leaving subscriber virtual machines configured with virtual NICS on this management Vlan can be very detrimental to a multi-tenant environment. It is a configuration detail that is often over looked. Even when access control lists are applied to the interfaces of the management Vlan that the hypervisor hosts are connected to, multiple customer environments on the same host will still be able to see one another because the traffic communicating on the management Vlan. This traffic never crosses the actual uplink interface (Hardware Nic of the physical host) because the virtual interfaces on the management Vlan communicate within the virtual environment in the same subnet. This is a misconfiguration that would not be stopped by any identity management solution, but is well worth mentioning in the context of this thesis because it is something that needs attention due to the false positives in the thesis results that this misconfiguration could create.

3.1.3 iSCSI Shared Storage

Virtual machines can be configured to run on local storage contained within the virtualization hosts in the environment. However, most of the high availability features of virtualization are only functional when shared storage is provided to the hosts. VMware's HA (High Availability) and VMotion (Allows live migrations of virtual machines between physical hosts) services are available when the hosts are connected to a storage area network (SAN) of some type. Many varieties of storage networking can be used. Fiber channel and iSCSI SANs are among the choices available.

Within this prototype environment a custom built iSCSI target is used. This iSCSI device is simply a 32-bit PC with a 500 gigabyte SATA drive installed running a software solution called Openfiler. Openfiler is an Open Source NAS/SAN solution and it comes with a wealth of features and capabilities that address specific storage management pain points. Openfiler management is performed via a powerful and intuitive web-based graphical user interface. Through this interface, various administrative tasks can be performed such as creating volumes, network shares, allocating disk quota for users and groups and managing RAID arrays [65].

The iSCSI device will be accessible to the cloud by through two network interfaces each in a different Vlan and security zone. One interface will be on the storage_vlan security zone (Vlan 80) and the other interface will be on the Home security zone (Vlan 1). Vlan 80 will be available to the interfaces on the VMware ESXi hosts that are configured to only communicate on the storage network to access iSCSI storage for the customer's virtual machines. A set amount of storage will be allocated to each subscriber depending on what level of service they purchase. Vlan 1 is a management Vlan that is only available to the cloud provider staff, then only to those administrative staff designated as storage administrators. Storage administrators will be designated by their user accounts being members of a storage administrators group in the prod.lan Active Directory domain. Openfiler can use LDAP to communicate with a directory service in order to use identity management to check access rights of a user account and assure only those

who are explicitly authorized to make storage changes will be allowed to even read configuration information on the storage device. This function of the storage management software will be examined more closely in the research.

3.1.4 Inside Network Routing and Switching

In this prototype environment, due to the small scale static routes will be used on all routers and firewalls. This is actually the most secure way to configure routing so that extraneous routes cannot be injected without routing protocols running. This best case scenario does not scale well. In real world larger implementations routing protocols must run to support the automation and size of the cloud. BGP is a protocol of choice due to its scalability and wide spread support on multi-vendor products.

One major drawback to using static routes is that it requires manual intervention by the IaaS cloud provider, even within the subscriber environment. This requires allowing provider access to the subscriber environment, so special care needs to be taken to limit this access to only the specific configuration tasks that are required and this access only be given to specific users who will be responsible for the initial setup of a subscriber's environment. This is yet another area where identity management will be of importance. Auditing of this function will be of high interest but would be useless without a solid identity management solution. This is an area of much concern for many companies contemplating the move to the cloud. There is not much assurance of trust that non-subscribers won't be able to meddle with the subscriber's networking environment intentionally or non-intentionally.

Automation supported by securely configured routing protocols alleviates some of the trust concerns surrounding the subscriber networking environment. A customer portal can be used to create a customer networking environment without the manual intervention of the cloud provider's networking team. This automation requires specialized and many times complex custom integrations that can introduce security issues of its own. These integrations require

custom code to be written against application APIs. The code itself can be written insecurely without proper input validation and passwords have been known to be hard coded and stored in clear text within log files. Even the APIs that are used have vulnerabilities and need to be constantly monitored and patched on a regular basis. A change control process becomes more important than ever because a patch or change that is not properly tested can bring down an entire customer environment inadvertently. Many security issues are due to integrations that focus on providing functionality without thinking of the security implications. Investigations into the details of these automation issues are outside the scope of this thesis and will be an area of future research.

3.1.5 VLAN Design

Here is a summary of the prototype IaaS Cloud Vlan design:

Vlan #	Network Address	Mask	Maximum # Addresses	Security Zone	Purpose
192	192.168.1.0	255.255.255.0	255	Internet	Internet
100	10.10.1.0	255.255.255.0	255	Home	Management Stack (AD, Tacacs, Security Tools, PKI, Log Aggregation
1	10.10.4.0	255.255.255.0	255	Work	Subnet for Vsphere Vcenters
70	10.10.7.0	255.255.255.0	255	Home	Active Directory for Customer Logins
80	10.10.8.0	255.255.255.0	255	N/A - Private Vlan	iSCSI Storage Network
	Customer Vlans				
1001	10.100.1.0	255.255.255.0	255	N/A	Customer Virtual Machines
1002	10.100.2.0	255.255.255.0	255	N/A	Customer Virtual Machines
	Untrust Subnet				
N/A	10.11.1.0	255.255.255.0	255	Untrust	Outside

Table 2: Vlan details of prototype environment

Vlans are used as security boundaries in this cloud in order to keep the customers from seeing each others' or the cloud infrastructure's data in this multi-tenant environment. There are multiple places where Vlan information is going to have to be configured. A consistent switching environment will have to be created throughout the entire IaaS cloud. To maintain consistency, the VLAN numbers are reflective of the defining octet value in the IP Network address. For

example in the class C subnet 10.10.4.0, the VLAN number is 1. And for 10.10.8.0, the VLAN number is 80. This loose patterning of the VLAN number after the ip addressing is for human readable purposes, to make the relationships easier to remember. No other significance is assigned to the VLAN numbers other than the fact that they are unique throughout this entire prototype environment.

The consistency will run from the outside firewalls on the edge, all the way down to the hypervisor level with the distributed virtual switches. The only way traffic will be allowed out of a Vlan will be through routed interfaces on internal routers or firewalls that exist in the environment. Even this traffic will be limited only to specific protocols which are needed by access control lists on interfaces and policy rules on firewall. Virtual switches managed by the hypervisors will maintain this Vlan integrity so that virtual machines from different customers that even reside on the same physical hardware will have their traffic remain separate.

As shown above, these Vlans also map to a concept called “security zones”. This mapping is noted due to the firewalls that are used in the environment. On many of the firewalls that are used in the prototype environment, security zones are logical entities to which one or more interfaces are bound. On a single device, you can configure multiple security zones, dividing the network into segments to which you can apply various security options to satisfy the needs of each segment. From the perspective of security policies, traffic enters into one security zone and goes out on another security zone. On the firewalls the only way traffic can flow from one security zone to another is if a route exists so that the traffic knows what interface to flow to and a security policy exists to allow the traffic from one zone to another. All of these Vlans and security zones are carefully planned to protect the infrastructure from outsiders and the customers as well as the customer environments from each other, outsiders and the cloud service provider. This configuration inherently trusts that the router or switch does not become compromised. Best

practices for securing routers and switches should be followed to ensure that trust. Logging and auditing should also be configured to monitor for any compromises.

In this prototype, the particular model of firewall allows up to three security zones. The use of these zones has been planned such that the control traffic to the ESXi servers is separated from the rest of the network traffic and all traffic is separated from an Untrust zone. In a public cloud, a more advanced firewall would be afforded that allows as many security zones required to segment traffic. These controls are but one of many access controls in place. The intimate details of the Vlan and security zone configurations are out of scope for this research.

3.1.6 Active Directory Domain #1 (prod.com)

A directory service is needed to store user credentials and map those credentials to a set of assigned access permissions. Any directory service could be used. Microsoft's Active Directory was used for this prototype because it is one of the most common directory services found in a network. This directory service will be the center piece of the identity management solution that will be used in this prototype IaaS Cloud. Active Directory will be responsible for authenticating and authorizing all users, computers and networking devices that operate on the cloud provider's network. This will not include the virtual machines that the subscribers own. There will be a separate Active Directory domain used to manage the set of subscriber users.

3.1.7 Active Directory Domain #2 (sub.com)

One of the primary precepts of this thesis involving identity management in a cloud is that there needs to be a separation of the directory services being used for the cloud provider and the subscribers using the services. This second Active Directory Domain (sub.lan) will be that second separate set of directory services for the subscribers. These user accounts are not the user accounts that the subscribers are creating to use on their own virtual servers. These user accounts are administrative user accounts that are assigned to each subscriber in order to manage their

virtual network containers on the cloud. They will use these accounts to log into an administrative virtual private network connection. They will also use these account to provision their own virtual machines and decommission their own virtual machines.

3.1.8 TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) is a Cisco Systems proprietary protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services [66]. The TACACS server will be used to authenticate administrators when they log onto routers and switches. The server is configured to use the domain controller in the prod.com domain for its credentials database. This will allow user accounts to be centrally maintained and audited as opposed to creating multiple sets of local credentials on each and every network device. This also makes regular password changes more manageable because only one account is maintained for each user.

3.1.9 Internal PKI

A Public Key Infrastructure will be maintained within the cloud. This will initially be used to issue trusted SSL certificates to web based administration and security tools in the IaaS infrastructure. It will also be used to provide certificates to subscribers so that they can use an administrative virtual private network connection to manage their virtual resources from the Internet. Smart cards will also be employed by provider administrative staff in order to perform maintenance activities on the infrastructure.

3.1.10 Patch/Update Servers

A major piece of the security strategy for any computing environment, more especially one as complex as an IaaS Cloud is resolving discovered security flaws by maintaining the most up to date, bug checked code available for all operating systems, protocols and applications. Most

major manufacturers (Microsoft, Cisco, VMware, etc.) make patch management more manageable by implementing automated patching capabilities. Microsoft and VMware both provide such facilities. Microsoft's patching functions are based on a technology called WSUS Services 3.0 and VMware has its vSphere Update Manager (VUM). WSUS uses .NET Framework, Microsoft Management Console and Internet Information Services. WSUS 3.0 uses either SQL Server Express or Windows Internal Database as its database engine [67]. VUM is a simple (Jetty) web server service and a download client. The update manager component is installed on a Windows 2003 or Windows XP machine that has access to the internet. It uses port 80 (443) to connect to the VMware (ESX) to obtain patch metadata [68].

3.1.11 Proxy/Reverse Proxy Server

The IaaS infrastructure itself is designed to be a closed network. None of the management components are directly exposed to the Internet. The only system that will be allowed Internet access through the external firewall is the proxy/reverse proxy server. The few systems that need consistent updates from the Internet will have their external communication proxied through this system. Any web based interfaces such as the cloud control portal will be reverse-proxied to the Internet through this system.

This will be a Windows 2003 server running Microsoft ISA 2004 software. The server will reside in its own work group. It will be a bastion host. A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application which in this case will be a proxy server, and all other services are removed or limited to reduce threats to the system. The reason for this hardening is that this system may involve access from un-trusted networks or computers [69]. The proxy server will be configured to send all of its log files to the syslog collection server (Splunk) so that traffic leaving the network can be examined. Using the proxy server in this manner will allow any proxied connections to be logged. The proxy rules are detailed here along with explanations:

ISA Firewall Policy							
Rule #	Rule Name	Action	Protocols	From	To	Condition	Notes
1	Ubuntu Admin	Allow	Http, Https, ICA, IKE Client, IPSec ESP, IPSEC NAT-T Client, L2TP Client, Ping PPTP, RDP, Rlogin, SSH, Telnet	Ubuntu Admin	Internal Net, Local Host	All Users	Allows administration from Ubuntu Admin Computer
2	Splunk Forwarder Rule	Allow	Splunk Forwarder, Syslog-514, Splunk Ports - (4454, 4480, 4497, 4507, 8089)	Local Host	Splunk	All Users	Allow ISA Server to send logs to Splunk Server
3	Splunk Access to ISA	Allow	All Outbound Traffic	Splunk	Local Host	All Users	Allow ISA Server to send logs to Splunk Server
4	Windows Update Site Access	Allow	All Outbound Traffic	Internal Net, Local Host	External	All Users	Needed for WSUS Service Updates
5	DNS Frowarding for prod.com	Allow	All Outbound Traffic	dc1.prod.com	External	All Users	allows primary dns server to service all of prototype
6	WSUS Update Rule	Allow	All Outbound Traffic	wsus.prod.com	External, windows update url list	All Users	Needed for WSUS Service Updates
7	MS-Update to WSUS	Allow	Http, Https	www.update.microsoft.com	wsus.prod.com	All Users	Needed for WSUS Service Updates
8	ACS Local	Allow	All Outbound Traffic	tacacs.prod.com	All Protected Nets, tacacs.prod.com, ACS Local url list	All Users	Allows workstations on prod network access to ACS login screen
9	Internet Access	Allow	All Outbound Traffic	tacacs.prod.com	External	All Users	Allows Screen router to use ACS
Last	Default Rule	Deny	All Traffic	All Nets	All Nets	All Users	Default Deny Any-Any Rule

Table 3: ISA firewall policy rules

3.1.12 Management Stack

The management stack is actually a name for a category of devices and not a specific device or piece of technology. It refers to the group of servers, applications and tools that will be used to manage and monitor the infrastructure of the IaaS cloud. Patch Servers, vulnerability scanners, change control monitoring devices, authentication servers, log collection and management servers, anti-virus management servers, IDS management stations, monitoring work stations, plus the switches and routers that provide connectivity to this layer.

These devices are used by and protected by the cloud provider administrators. Not only are these tools used to monitor the cloud infrastructure, but they are part of that very infrastructure that needs to be watched. The subscribers need to be assured that the staff with administrative access is not abusing these powerful tools to monitor customer traffic. This is one of the areas where the study of identity management and access controls is very important. Without strictly kept access controls and identity management, there would be no way to assure

the customers of this confidence and no way to hold these administrative people with super user status accountable for any breaches due to insider threats.

3.1.13 VPN Access

Virtual Private Network connections (VPN) will be used to provide any customer management access to their virtual machines in the cloud. SSL VPNs will be used for a customer to remotely manage their virtual resources. Site to site IPSec VPNs will be used to connect their virtual resources to their own customer premise network. When a customer chooses to create externally facing systems, the customer can rely on local authentication account to provide identity management on the system or, they can buy publicly available certificates and services from a company like VeriSign. A third option would involve the cloud provider extending their own PKI and identity management systems in order to provide an additional service for the customer.

Customers can buy resources from the IaaS cloud provider such that they are externally facing to the Internet, or they can buy resources that will remain private and not have a publicly routable IP address. This is typically where they would use a site to site VPN connection to their own infrastructure. These cases provide ample opportunity for the IaaS cloud provider to integrate the identity management solutions that are presented in this document. The IaaS may have an identity management system that can extend into the customer premise environment or the customer may choose to rely on whatever identity management system they currently run in their own environment.

3.1.14 Cloud Control and Management

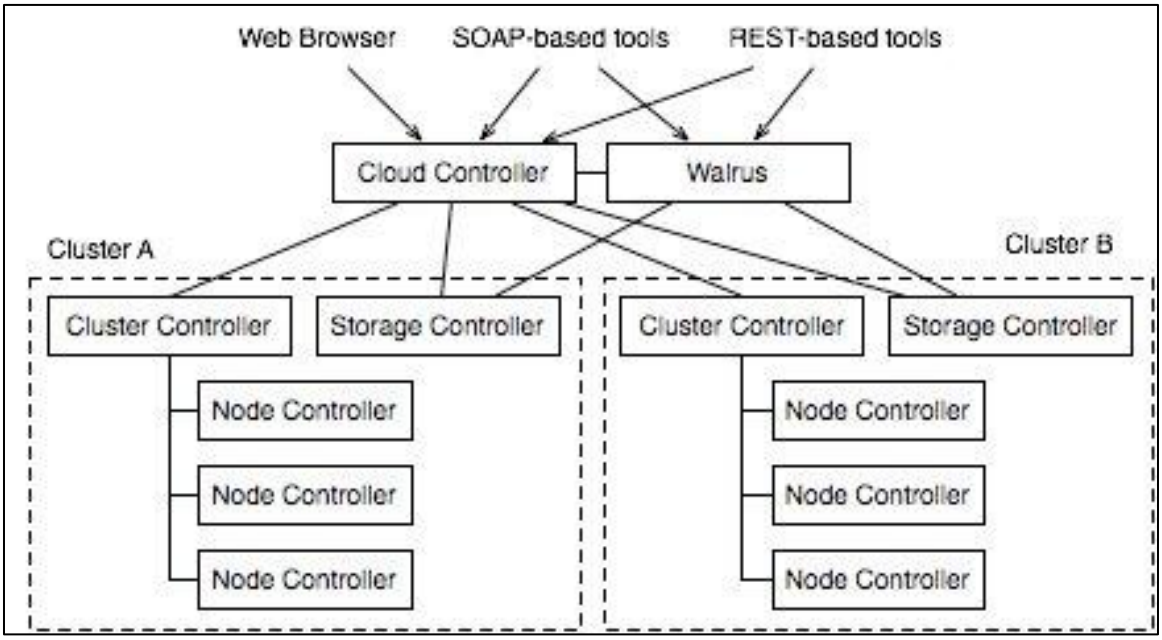

Figure 3: Logical Components of Eucalyptus Cloud Control Portal

Eucalyptus will be used for the cloud control and resource scheduling component. A Eucalyptus cloud setup consists of five types of components. The cloud controller (CLC) and "Walrus" are top-level components, with one of each in a cloud installation. The cloud controller is a Java program that offers EC2-compatible SOAP and "Query" interfaces, as well as a Web interface to the outside world. In addition to handling incoming requests, the cloud controller performs high-level resource scheduling and system accounting. Walrus, also written in Java, implements bucket-based storage, which is available outside and inside a cloud through S3-compatible SOAP and REST interfaces [70]. Below is a diagram of the Eucalyptus architecture:

3.1.15 Firewall

The firewall being used in the prototype is a Juniper NetScreen-5 GT. This model is the most basic model firewall that Juniper offers, but serves the basic required services of a firewall in this prototype. This firewall is configured in route mode with Network Address Translation

(NAT) enabled. Juniper also introduces the idea of security zones. A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies [71]. Security zones are logical entities to which one or more interfaces are bound. The NetScreen device acts as a router and a firewall. It separates three internal networks, 10.10.1.0/24,10.10.4.0/24 and 10.10.7.0/24 from the untrusted network 10.11.1.0/24. The rest of the networks in the prototype remain internal and have no reason to send traffic through the firewall.

Each network is assigned to an interface on the NetScreen. Interfaces act as a doorway through which traffic enters and exits the device. Many interfaces can share the same security requirements. These interfaces that can share the same security requirements are assigned to the same security zone. For example, in this prototype, the networks 10.10.1.0/24 and 10.10.7.0/24 share the same requirements so they will be assigned to the same security zone. Whereas, the network 10.10.4.0, containing the management interfaces of the ESXi servers, has a different set of security requirements, will be placed in a different security zone. Each time traffic is routed through the firewall, the zone location for the source and destination interfaces is checked. If the path traverses a security zone, then the traffic must also have a security policy that allows the traffic to pass. If the source and destination interfaces do not cross security zones than the only thing required is a route.

On this firewall, three security zones exist: Home, Work and Untrust. These are default security zones for this device. By default, polices are configured such that traffic from Home to Untrust and Work to Untrust flow freely. Work to Home flows freely, yet Home to Work is blocked by policy. This default behavior governed which networks were assigned to each zone. The Untrust zone was used for all networks outside the prototype. The Work zone was used for the management network of the ESXi hosts. All other internal networks were assigned to the Home zone. Since a major goal is to protect the ESXi management network from all other traffic it made sense to place that network in the Work zone. The Home zone is used to apply the same

firewall policies to all of the other internal networks. In a production environment, a different model of firewall would be used which allows the creation of additional security zones for more customized security policies.

For simplicity purposes in this prototype environment, the firewall rules were kept to a minimum in order to allow basic functionality to test some of the misuse cases and demonstrate some of the core portions of the identity management solution being proposed. Firewalls are a very important technical security control in a cloud, but not the control that is being studied in this research. In a production environment, firewall rules would be much more granular than those present here, specifically allowing just those protocols needed for communication between specific destinations. All rules are configured to log when network traffic matches the rule in order to monitor all traffic through the firewall, allowed or denied. The firewall rules on the NetScreen firewall are listed below:

NetScreen Firewall Policies						
From Work To Untrust - 1 Policy						
ID	**Source**	**Destination**	**Service**	**Action**	**Log**	**Notes**
1	Any	Any	Any	Allow	Yes	Default
From - Work to Home - 2 Policies						
ID	**Source**	**Destination**	**Service**	**Action**	**Log**	**Notes**
5	10.10.4.5/32	10.10.1.0/24	PING	Allow	Yes	Testing
2	Any	Any	Any	Allow	Yes	Default
From Home To Untrust - 1 Policy						
ID	**Source**	**Destination**	**Service**	**Action**	**Log**	**Notes**
3	Any	Any	Any	Allow	Yes	Default
From Home To Work - 1 Policy						
ID	**Source**	**Destination**	**Service**	**Action**	**Log**	**Notes**
4	Any	Any	Any	Deny	Yes	Default
From - Untrust to Home - 3 Policies						
ID	**Source**	**Destination**	**Service**	**Action**	**Log**	**Notes**
7	10.11.1.0/24	10.10.1.5/32	SYSLOG	Allow	Yes	Splunk
6	10.11.1.254/32	10.10.15/32	ANY	Allow	Yes	Splunk
8	10.11.1.1/32	10.10.1.0/24	PING	Allow	Yes	IDS Testing
From - Untrust to Home - 3 Policies						
ID	**Source**	**Destination**	**Service**	**Action**	**Log**	**Notes**
9	10.11.1.0/24	10.10.4.0/24	Any	Allow	Yes	Screen Router Testing Purposes

Table 4: NetScreen firewall policy rules

3.1.16 Internet Access

Internet access will only be allowed to the customer's externally facing virtual machines, the cloud control portal web page and administrative systems that need updates from vendors. Customer externally facing virtual machines will be given Internet access by providing their virtual machines with IP addresses that are publicly routed to the Internet. Any IaaS management web pages that need to be externally facing will be reverse proxied by the proxy server. Systems that will need vendor updates such as patches, anti-virus definitions and IDS signatures will be forced to obtain their updates through the proxy server which will limit their Internet access to the specific servers that they need to reach in order to obtain their updates.

3.1.17 Snort Intrusion Detection Sensor

There is a Snort intrusion detection device monitoring the Untrust network between the screen router and the NetScreen firewall and ISA proxy server. Snort is installed on a server with the Ubuntu LTS 10.04 operating system released in April 2010 which is supported until April 2013. It is currently running a signature set from January 2012 to detect anomalies. It is configured to write alerts to a local log file as well as send them via syslog to the centralized syslog server on the network. Barnyard is also installed which is a Snort plunging that offloads the reporting function to make the Snort IDS function more efficient.

3.1.18 Splunk – Syslog Collector and Correlation

All device and server audit and application logs are forwarded via syslog to a centralized log collection server. The Splunk server is the key component to the auditing functions of the prototype. All devices and servers are configured via syslog or the use of an agent to collect all logging activity and send it to the Splunk server. Splunk understands the format of all the various log formats and indexes all of the information found so that it is more easily searchable and

correlated. Search queries can be created to associate log entries from various sources together into one event. An event can then be analyzed and used to understand what is occurring in the environment.

3.2 Procedures

Each of these misuse cases has several different scenarios that can be walked through. In each section, the various scenarios are briefly described with the related actors, threats, mitigations and paths. One scenario will be chosen from each of the misuse cases and simulated. The simulation steps performed in the prototype for each misuse case will be detailed within each relevant procedures section (3.2.1 – 3.2.4). All related audit log files will be collected, correlated and analyzed after each simulation. Those results will be presented and discussed each relevant results and analysis sections.

Due to limitations of prototype environment, the rogue virtual machine was assigned a virtual network card that is connected to the hypervisor network. The purpose of these tests are to see if identity management provides attack mitigation, not to test the switching and networking security of the environment.

3.2.1 Misuse Case #1 Details and Procedures

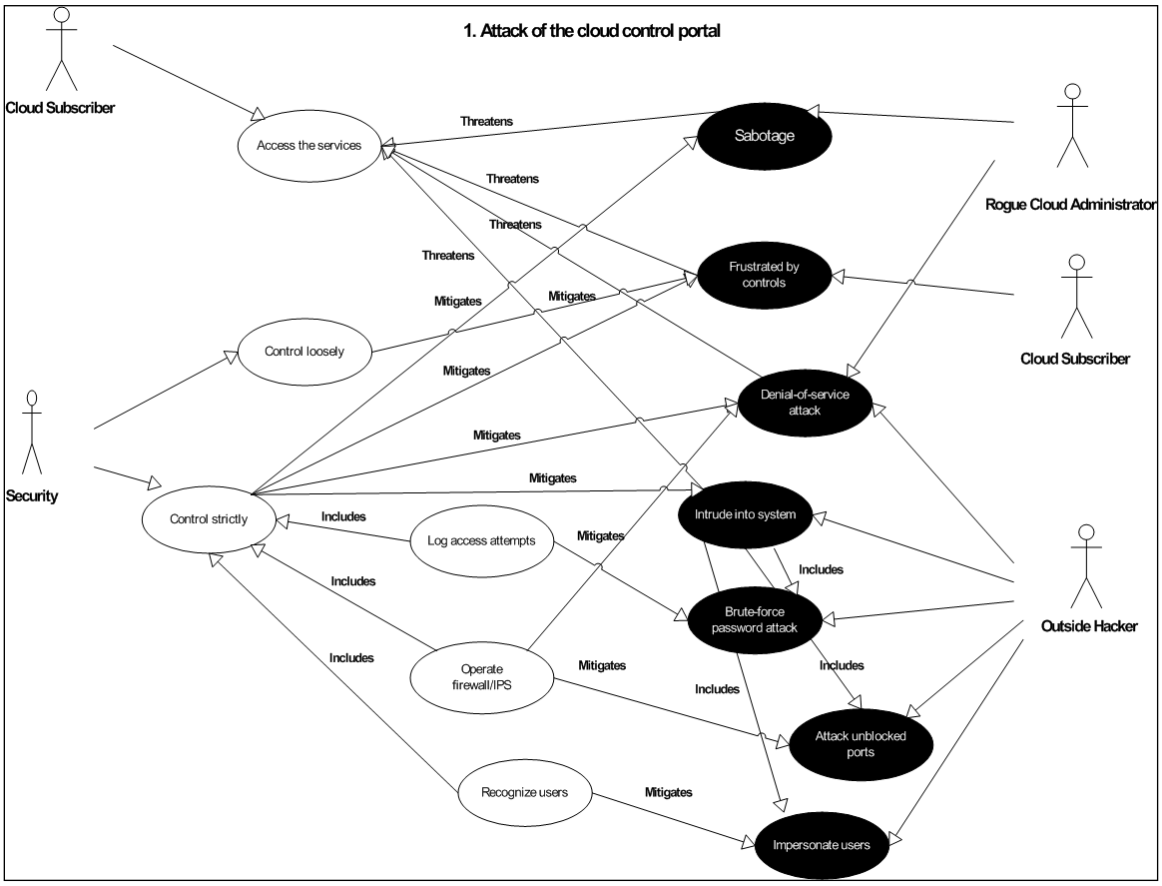

Figure 4: Misuse Case #1 – Attack of the cloud control portal

Attack of the cloud control portal

These misuse cases cover internal and external attack vectors to the cloud control portal that customers typically use to manage the virtual environment that they lease from the IaaS Cloud

Scenario:	Denial of Service Attack on the portal (DoS Attack)
Triggering event:	DoS Attack targeting services provided to customers through the portal

Actors:	Rogue Cloud Administrator, Outside Hacker
Related misuse cases:	Sabotage, Frustrated by controls, Intrude into system, Brute-force password attack, Attack unblocked ports, Impersonate users.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Attacker successfully launches Denial of Service Attach such that the Cloud Subscriber will not have access to the Portal Services to control his virtual infrastructure.
Basic Path:	BP1 – Attacker creates and launches TCP/SYN packets with forged sender address BP2 – Attacker sends forged packets to cloud control portal BP3 – The SYN flood packets spawn a lot of half-open connections on the cloud control portal. BP4 – Half-open connections saturate the number of connections cloud control portal can make. BP5 – Cloud control portal can no longer service requests from the Cloud Tenants. BP6 – Cloud Tenants can no longer manage their virtual infrastructure.
Alternate Paths:	AP1 – in action 1 attacker can launch Smurf Attack against Cloud Control Portal by sending malformed packets with the cloud control portal ip address as the source address to the broadcast address of the network.
Mitigation Path	MP1 – in action 1 the IaaS Security Services Operate firewall/IDS device to intercept and block DoS traffic before it gets to the Cloud Control Portal. MP2 – in action 1 network devices are strictly configured to filter traffic such that communication to the broadcast address Is not replied to. MP3 – in action 2 access attempts on the Cloud are logged so when attack is sourced within the cloud, the Security team can track down the source and stop the attack.

Table 5: Denial of Service Attack on the portal

Scenario:	Cloud Subscriber is frustrated by the strict security controls in the cloud
Triggering event:	Cloud subscriber attempts to circumvent security controls that restrict services available through the Cloud Control Portal.
Actors:	Cloud Subscriber
Related misuse cases:	Sabotage, Denial of Service Attack, Intrude into system, Brute-force password attack, Attack unblocked ports, Impersonate users.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Frustrated Cloud Subscriber will have circumvented the security controls of the Cloud Control Portal and will able to perform functions that were previously denied.
Basic Path:	BP1 – Cloud Subscriber launches a virtual machine in their environment to listen to passing network traffic. BP2 – Subscriber obtains configuration information about portal through recon activities. BP3 – Subscriber uses learned knowledge to make setting changes to his user rights and gain more privileges.
Alternate Paths:	No Alternate Paths.
Mitigation Path	MP1 – in action 3 security services logs access attempts and verifies any changes to configuration found. MP2 – in action 3 security services reverts any unapproved setting changes back to last approved baseline.

Table 6: Cloud Subscriber is frustrated by the strict security controls in the cloud

Scenario:	Rogue Cloud Administrator Sabotages the Cloud Control Portal
Triggering event:	Rogue Administrator uses elevated privileges to attack the Cloud Control Portal
Actors:	Rogue Cloud Administrator
Related misuse cases:	Denial of Service Attack, Frustrated by controls, Intrude into system, Brute-force password attack, Attack unblocked ports, Impersonate users.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Rogue Cloud Administrator successfully commits sabotage and damages the services of the Cloud Control Portal such that the Cloud Subscribers can't use it.
Basic Path:	BP1 – Attacker uses his own elevated credentials. BP2 – Launches Direct Attack on Cloud Control Portal BP3 – Attacker removes evidence of attack.
Alternate Paths:	No alternate Path
Mitigation Path	MP1 – In action 1 Identity Management and Auditing log access attempts allow IaaS Security services to track down the actions of the Rogue Cloud Administrator. MP2 – In action 3 the logging of access attempts and auditing store the logs remotely and securely so that even administrators with elevated privileges can't alter the logs.

Table 7: Rogue Cloud Administrator Sabotages the Cloud Control Portal

Scenario:	Outside Hacker Intrudes into the Cloud Control Portal
Triggering event:	Attacker attempts to intrude into Cloud Control Portal
Actors:	Rogue Cloud Administrator, Outside Hacker
Related misuse cases:	Sabotage, Frustrated by controls, Intrude into system, Brute-force password attack, Attack unblocked ports, Impersonate users.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Attacker successfully gains access to cloud control portal and can uses and manipulate services to affect the Cloud Subscribers or IaaS Infrastructure.
Basic Path:	BP1 – Attacker uses hacking tools to launch malicious code from a computer on the Internet. BP2 – Malicious code targets vulnerabilities of Cloud Control Portal. BP3 – Reverse shell is spawned from Cloud Control Portal to attacker that allows access.
Alternate Paths:	AP1 – In action 3, the attacker launches Brute Force password attack to gain credentials and get elevated privileges by gaining a password to an administrative user account on the Cloud Control Portal. AP2 – In action 2, the malicious code launches attacks on unblocked ports on the Cloud Control portal to gain access to the system. AP3 – After action 3, attacker uses brute forced passwords to impersonate system users on the Cloud Control Portal to gain access to Cloud Subscriber services.
Mitigation Path	MP1 – In action 2 of the Basic Path the IaaS Security Services Operate firewall/IDS device to block traffic targeted for unblocked ports. MP2 – In action 2 when port is unblocked by firewall, IDS alerts of attack type packet flowing through open port and blocks suspicious behavior. MP3 – in action

	3 of the Alternate Path, Identity Management solution that recognizes users allows IaaS Security Services to recognize impersonated users and stop the attack. MP4 – in action 3, Identity Management and Auditing log access attempts allow IaaS Security services to track down and stop Brute-force password attacks.

Table 8: Outside Hacker Intrudes into the Cloud Control Portal

The scenario that was run in the prototype environment for this use case was a denial of service attack (DOS) on the cloud control portal. The DOS attack will be launched by a disgruntled cloud administrator who just found out he is about to lose his job. The following is merely a description of the scenario and the steps taken to simulate it in the prototype environment. The analysis of the mitigations of this attack is discussed in the results and analysis section of this thesis.

Denial of Service Attack on the portal - Procedure

1. Tenant has launched a rogue virtual machine into its virtual network container that has hacking tools installed on it.
2. The set up of the rogue virtual machine in the subscriber's container is only slightly more trivial in this prototype then it would be in a production IaaS Cloud.
3. Open https://10.10.4.33 in a web browser successfully to prove that the portal web site was up and running properly. It was.
4. Python script "slowloris.pl" (source http://ha.ckers.org/slowloris.pl) was run to create a DoS attack against the https interface of the ESXi hypervisor that holds guest virtual machines.
5. Command to run “script: ./slowloris.pl -dns 10.10.4.33 -port 443 -timeout 30 -num 500 –https”

6. With the DoS script running I opened https://10.10.4.33 in a web browser and the site would not respond.

7. The DoS script was stopped.

8. Finally, Open https://10.10.4.33 in a web browser successfully, to prove site was again responding as usual.

3.2.2 Misuse Case #2 details and procedures

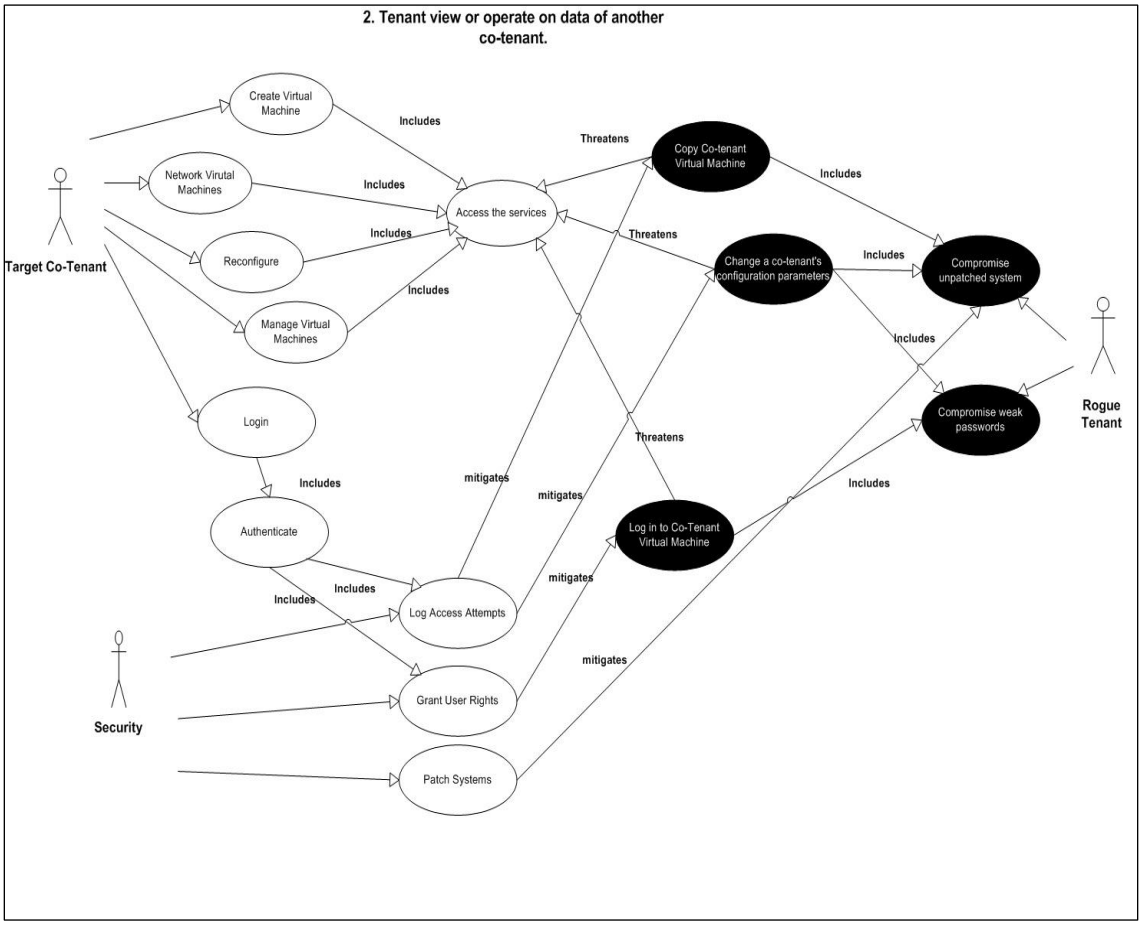

Figure 5: Misuse Case #2 – Tenant view or operate on data of another co-tenant.

Tenant view or operate on data of another co-tenant

These misuse cases cover situations where a rogue tenant on the IaaS C loud could view or operate on data in another co-tenant's virtual network.

Scenario:	Copy a co-tenant's virtual machine
Triggering event:	Rogue tenant is able to break out of their own virtual machine and compromise unsecured systems to copy another customer's virtual machine.
Actors:	Rogue Tenant
Related misuse cases:	Change a co-tenant's configuration parameters, Log into co-tenant virtual machine
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Attacker successfully copies another customer's virtual machine such that they are able to mount it offline somewhere else and steal all of the data off of it.
Basic Path:	BP1 – Attacker creates virtual machine in their assigned environment to launch attacks from. BP2 – Attacker uses hacking tools or launches malicious script. BP3 – Attack breaks out of the hypervisor to use the underlying infrastructure. BP4 – through underlying infrastructure, Attacker accesses another tenant's virtual machine. BP5 – Attacker is able to copy the virtual hard drive files of another tenant's virtual machine. BP6 – Attacker can mount the virtual hard drive files off-line and power up the copy of the virtual machine to get data from the co-tenant virtual machine.

Alternate Paths:	AP1 – in action 3 attacker takes advantage of un-patched hypervisors in the IaaS cloud in order to break out of the hypervisor.
Mitigation Path	MP1 – in action 3 the hypervisors that have been patched by the IaaS Security team are not vulnerable to attacks that avoid authentication methods. MP2 – in action 4 the Identity Management Solution implemented by the IaaS Security team along with auditing logs all access attempts and notifies the security team of malicious activity that is occurring so that it can be tracked down and stopped.

Table 9: Copy a co-tenant's virtual machine

Scenario:	Change a co-tenant's configuration parameters
Triggering event:	Cloud subscriber attempts to circumvent security controls that restrict services available through the Cloud Control Portal.
Actors:	Cloud Subscriber
Related misuse cases:	Sabotage, Denial of Service Attack, Intrude into system, Brute-force password attack, Attack unblocked ports, Impersonate users.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Frustrated Cloud Subscriber will have circumvented the security controls of the Cloud Control Portal and will able to perform functions that were previously denied.

Basic Path:	BP1 – Cloud Subscriber launches a virtual machine in their environment to listen to passing network traffic. BP2 – Subscriber obtains configuration information about portal through recon activities. BP3 – Subscriber uses learned knowledge to make setting changes to his user rights and gain more privileges.
Alternate Paths:	No Alternate Paths.
Mitigation Path	MP1 – in action 3 security services logs access attempts and verifies any changes to configuration found. MP2 – in action 3 security services reverts any unapproved setting changes back to last approved baseline.

Table 10: Change a co-tenant's configuration parameters

Scenario:	Log into a co-tenant's virtual machine.
Triggering event:	Rogue Administrator uses elevated privileges to attack the Cloud Control Portal
Actors:	Rogue Cloud Administrator
Related misuse cases:	Denial of Service Attack, Frustrated by controls, Intrude into system, Brute-force password attack, Attack unblocked ports, Impersonate users.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Rogue C loud Administrator successfully commits sabotage and damages the services of the Cloud Control Portal such that the Cloud Subscribers

	can't use it.
Basic Path:	BP1 – Attacker uses his own elevated credentials. BP2 – Launches Direct Attack on Cloud Control Portal BP3 – Attacker removes evidence of attack.
Alternate Paths:	No alternate Path
Mitigation Path	MP1 – In action 1 Identity Management and Auditing log access attempts allow IaaS Security services to track down the actions of the Rogue Cloud Administrator. MP2 – In action 3 the logging of access attempts and auditing store the logs remotely and securely so that even administrators with elevated privileges can't alter the logs.

Table 11: Log into a co-tenant's virtual machine

The scenario that was run in the prototype environment for this use case was a cloud tenant attempting to copy another tenant's virtual machine. The copy attempt will be launched by a tenant who creates a malicious virtual machine with hacking tools. They will use the administrative user account that has been assigned to them by the cloud provider to attack their neighbor.

Copy a co-tenant's virtual machine - Procedure

1. Tenant has launched a rogue virtual machine into its virtual network container with hacking tools installed on it.
2. Launch Metasploit within the BACKTRACK 5 customer virtual machine.
3. Called the "vmware_guest_stealer.rb" Vasto module, set remote host to the vmware host where other customer virtual machines are stored (esxi3.prod.com - 10.10.4.33) and launched the exploit.

4. The exploit failed due to a vulnerability patch already being applied to esxi3.prod.com. Had the exploit been successful, the attack would not be detected because of the limited audit and logging visibility into the subscriber's virtual environment.

3.2.3 Misuse Case #3 details and procedures

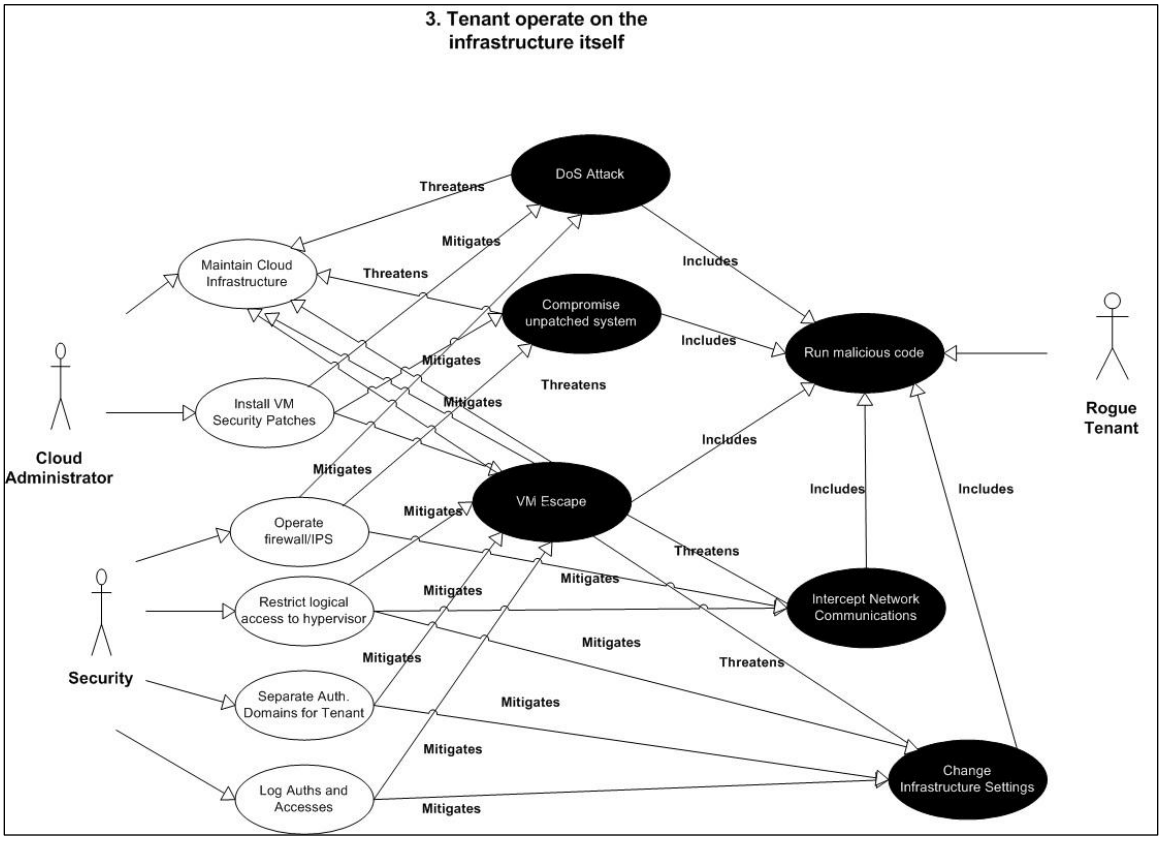

Figure 6: Misuse Case #3 – Tenant operate on the infrastructure itself

Tenant operate on the infrastructure itself

These misuse cases cover attack vectors related to a rogue tenant on the IaaS Cloud trying to operate on the cloud infrastructure itself.

Scenario:	Denial of Service Attack on the IaaS infrastructure
Triggering event:	DoS Attack from a tenant targeting the IaaS infrastructure
Actors:	Rogue tenant
Related misuse cases:	Compromise un-patched systems, Virtual Machine Escape, Change infrastructure settings, Tap Communications
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Attacker successfully launches Denial of Service Attach such that an IaaS infrastructure component gets saturated and cannot service customers.
Basic Path:	BP1 – Rogue tenant is able to run malicious code from a virtual machine that can pass traffic to underlying hardware. BP2- Attacker launches creates TCP/SYN packets with forged sender address BP2 – Attacker sends forged packets to any architecture component that is found that it can communicate with. BP3 – The SYN flood packets spawn a lot of half-open connections on the infrastructure. BP4 – Half-open connections saturate the number of connections architecture can make. BP5 – architecture component can no longer service requests from the Cloud Tenants or cloud administrators. BP6 – Cloud Tenants issues managing their virtual infrastructure.
Alternate Paths:	AP1 – in action 2 attacker can launch Smurf Attack against architecture by sending malformed packets with the cloud control portal ip address as the source address to the broadcast address of the network.

Mitigation Path	MP1 – in action 1, logical access to the hypervisor is restricted by the IaaS Security team to mitigate tenant access to the underlying infrastructure. MP2 – in action 1 the Cloud Administrator applies patches to systems to mitigate virtual machine breakout and other vulnerabilities. MP3 – in action 2 the IaaS Security Services Operate firewall/IDS device to intercept and block DoS traffic before it gets to the infrastructure components.

Table 12: Denial of Service Attack on the IaaS infrastructure

Scenario:	Compromise un-patched systems
Triggering event:	Rogue tenant is able to break out of their virtual machine and compromise un-patched systems in the IaaS cloud infrastructure
Actors:	Rogue Tenant
Related misuse cases:	Denial of Service Attack on the IaaS infrastructure, Virtual Machine Escape, Change infrastructure settings, Tap Communications
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Rogue tenant has been able to compromise an un-patched component of the IaaS infrastructure.
Basic Path:	BP1 – a rogue tenant performs discovery activities and finds vulnerable piece of IaaS infrastructure. BP2 - a rogue tenant launches malicious code. BP3 – code targets vulnerable IaaS infrastructure component. BP4 – malicious code compromises infrastructure component. BP5 – rogue tenant establishes access

	to infrastructure component and negatively affects the ability of the cloud administrators to manage the infrastructure.
Alternate Paths:	No Alternate Paths.
Mitigation Path	MP1 – in action 1, logical access to the hypervisor is restricted by the IaaS Security team to mitigate tenant performing discovery outside their virtual network.. MP2 – in action 1 the Cloud Administrator applies patches to systems to mitigate virtual machine breakout and other vulnerabilities. MP3 – in action 2 the IaaS Security Services Operate firewall/IDS device to intercept and block traffic before it gets to the infrastructure components. MP4 – in step 5, the IaaS Security team log authentications and accesses mitigates rogue tenant accesses on infrastructure components.

Table 13: Compromise un-patched systems

Scenario:	Virtual Machine Escape
Triggering event:	Rogue tenant is able to take advantage of un-patched hypervisor and break out of their virtual machine to perform nefarious actions.
Actors:	Rogue Tenant
Related misuse cases:	Denial of Service Attack on the IaaS infrastructure, Compromise un-patched systems, Change infrastructure settings, Tap Communications.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition

Post-condition:	Rogue tenant is able to take advantage of an un-patched hypervisor and "Breakout" such that he can perform communications and operations outside of their assigned virtual network.
Basic Path:	BP1 – a rogue tenant performs discovery activities and finds vulnerable hypervisor. BP2 - a rogue tenant launches malicious code. BP3– malicious code compromises hypervisor to allow the rogue tenant to operate directly through the hypervisor. BP4 – rogue tenant now able to reach areas of the infrastructure outside their own virtual network.
Alternate Paths:	No alternate Path
Mitigation Path	MP1 – in action 1, logical access to the hypervisor is restricted by the IaaS Security team to mitigate tenant performing discovery outside their virtual network.. MP2 – in action 3 the Cloud Administrator applies patches to systems to mitigate virtual machine breakout and other vulnerabilities. MP3 – in step 3, the IaaS Security team restrict logical access to the hypervisor mitigates any direct manipulation of the hypervisor from a hosted virtual machine. MP4 – in step 4, the IaaS Security team log authentications and accesses mitigates rogue tenant accesses on infrastructure components.

Table 14: Virtual Machine Escape

Scenario:	Change infrastructure settings
Triggering event:	Rogue tenant is able to break out of virtual machine and make changes to the IaaS infrastructure.
Actors:	Rogue Tenant
Related misuse cases:	Denial of Service Attack on the IaaS infrastructure, Compromise un-patched systems, Virtual Machine Escape, Tap Communications.

Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Rogue tenant is able to break out of virtual machine and make changes on devices in the IaaS infrastructure.
Basic Path:	BP1 – a rogue tenant performs discovery activities and finds vulnerable hypervisor. BP2 - a rogue tenant launches malicious code. BP3– malicious code compromises hypervisor to allow the rogue tenant to operate directly through the hypervisor. BP4 – rogue tenant now able to reach areas of the infrastructure outside their own virtual network.
Alternate Paths:	No alternate Path
Mitigation Path	MP1 – in action 1, logical access to the hypervisor is restricted by the IaaS Security team to mitigate tenant performing discovery outside their virtual network.. MP2 – in action 3 the Cloud Administrator applies patches to systems to mitigate virtual machine breakout and other vulnerabilities. MP3 – in step 3, the IaaS Security team restrict logical access to the hypervisor mitigates any direct manipulation of the hypervisor from a hosted virtual machine. MP4 – in step 4, the IaaS Security team log authentications and accesses mitigates rogue tenant accesses on infrastructure components.

Table 15: Change infrastructure settings

Scenario:	Intercept IaaS Infrastructure Network Communications
Triggering event:	Rogue tenant is able to tap communications from outside their assigned virtual network. (Vlan)
Actors:	Rogue Tenant

Related misuse cases:	Denial of Service Attack on the IaaS infrastructure, Compromise un-patched systems, Virtual Machine Escape, Change infrastructure settings.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Rogue tenant is able to listen in on communications that are occurring on the IaaS infrastructure.
Basic Path:	BP1 – Rogue tenant launches malicious code. BP2 – Malicious code breaks out of hypervisor. BP3 – Rogue tenant is able to launch man in the middle attacks on the IaaS infrastructure.
Alternate Paths:	No alternate Path
Mitigation Path	MP1 – In action 2, the IaaS Security Team restricts logical access to hypervisor to mitigate hypervisor breakout. MP2 – in step 2, the IaaS Cloud Administrator install VM Security Patches mitigates the breakout of the hypervisor. MP3 – In action3 the IaaS Security Team operates firewall/IPS to mitigate man in the middle attacks.

Table 16: Intercept IaaS Infrastructure Network Communications

The scenario that was run in the prototype environment for this use case was an attempt by a rogue tenant to change the settings of a piece of infrastructure equipment in the IaaS Cloud. The attempt will be made using the administrative user account that has been provided to the tenant by the IaaS cloud provider.

Change infrastructure settings - Procedure

1. Leaps of faith made with subscriber's access rights for demonstration purposes.

1. A subscriber administrator has logged into an ESXi management console.

2. The subscriber administrator powers down another subscriber's virtual machine from the management console.

3. The subscriber administrator logs out of the management console.

3.2.4 Misuse Case #4 details and procedures

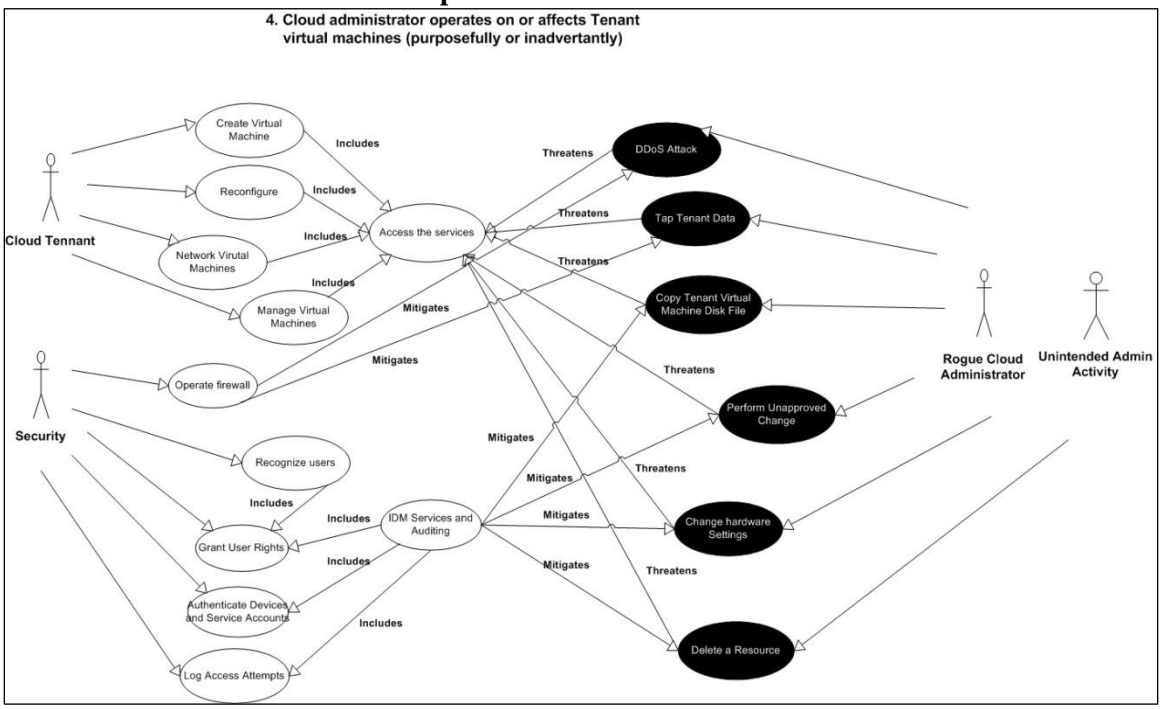

Figure 7: Misuse Case #4 – Cloud administrator operates on or affects Tenant Virtual Machine

Cloud admin operates on or affects tenant virtual machines (purposefully or inadvertently)

These misuse cases cover situations where a rogue Cloud Administrator or unintentional Cloud Admin activities affect a tenant on the IaaS Cloud.

Scenario:	DDos Attack
Triggering event:	Purposeful DoS attack from a rogue Cloud administrator or inadvertent act from a cloud administrator that saturates a resource in the Cloud and causes a DoS condition for the services that the subscribers depend on..
Actors:	Rogue Cloud Administrator, Unintended Admin Activity

Related misuse cases:	Tap Tenant Data, Copy Tenant Virtual Machine Disk File, Perform unapproved change, Change hardware settings ,Delete a resource.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Attacker successfully launches Denial of Service Attach such that an IaaS infrastructure component gets saturated and cannot service customers.
Basic Path:	BP1 - Unintended Administrative activity may accidentally over subscribe a resource such that it negatively affects the availability of the services available to the cloud tenant. BP2 – Rogue Admin is able to run malicious code from a virtual machine or computer in the IaaS infrastructure that can pass traffic to underlying hardware. BP3- Attacker launches creates TCP/SYN packets with forged sender address BP4 – Attacker sends forged packets to any architecture component that is found that it can communicate with. BP5 – The SYN flood packets spawn a lot of half-open connections on the infrastructure. BP6 – Half-open connections saturate the number of connections architecture can make. BP7 – architecture component can no longer service requests from the Cloud Tenants or cloud administrators. BP6 – Cloud Tenants have issues managing their virtual infrastructure.
Alternate Paths:	AP1 – in action 3 attacker can launch Smurf Attack against architecture by sending malformed packets with the cloud control portal ip address as the source address to the broadcast address of the network.
Mitigation Path	MP1 – in action 1, the IaaS Security team IDM Services and Auditing track which admin is making the offending changes and mitigates with a resolution. MP2 – in action 2 the hypervisors that have been patched by the IaaS Security team are not vulnerable to attacks that avoid authentication methods. MP2 – in action 3 the Identity Management Solution implemented by the IaaS Security team along with auditing logs all access attempts and notifies the security team of malicious activity that is occurring so that it can be tracked down and stopped.

Table 17: DDos Attack

Scenario:	Tap Tenant Data
Triggering event:	Rogue Cloud administrator is able to capture tenant data and take it off the network or just use it for purposes outside any agreements made between the tenant and the IaaS Cloud. Cloud administrative activity could also cause an unintended data leak from the tenant environment.
Actors:	Rogue Cloud Administrator, Unintended Admin Activity.
Related misuse cases:	DDos Attack, Copy Tenant Virtual Machine Disk File, Perform unapproved change, Change hardware settings , Delete a resource.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Intentional or unintentional data leak has occurred from the tenant environment.
Basic Path:	BP1 – Rogue Cloud Administrator has administrative rights to capture data from tenant environment. BP2 – Unintended administrative activity has rights to change environment. BP3 – changes to infrastructure can lead to an unintended data leak.
Alternate Paths:	No Alternate Paths.
Mitigation Path	MP1 – in action 1 IaaS Security grant user rights included in the IDM. Services and Auditing mitigate rogue cloud administrators tapping client data by enforcing separation of duties through the user rights and logging access attempts. MP2 – in action 2, IaaS Security IDM Services and Auditing mitigate unintended changes by limiting who can make them and limits who can leak what data and track what data may have been leaked to

	be a detective control during incident response.

Table 18: Tap Tenant Data

Scenario:	Copy Tenant Virtual Machine Disk File.
Triggering event:	Rogue Cloud Administrator abuses access rights to copy a tenant virtual machine disk file and take it off of the network for nefarious purposes.
Actors:	Rogue Cloud Administrator
Related misuse cases:	DDos Attack, Tap Tenant Data, Perform unapproved change, Change hardware settings , Delete a resource.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Tenant data is leaked due to Cloud Administrator copying the virtual hard drive of a client virtual machine off of the network.
Basic Path:	BP1 – Rogue Cloud administrator uses administrative rights and management utilities to copy a tenant's virtual machine. BP2 – Cloud Administrator puts copied files on removable storage to take off of network.
Alternate Paths:	No alternate Path
Mitigation Path	MP1 – in action 1 IaaS security enforce separation of duties through IDM Services and Auditing. MP2 – Granting User Rights is used to restrict Administrator from copying virtual machine hard disk files off of the

	network.

Table 19: Copy Tenant Virtual Machine Disk File

Scenario:	Perform unapproved change
Triggering event:	Cloud Administrator makes configuration change to devices on the IaaS that are not approved. These changes negatively impact the tenant environment.
Actors:	Unintended Administrative Activity, Rogue Cloud Administrator.
Related misuse cases:	DDos Attack, Tap Tenant Data, Copy Tenant Virtual Machine Disk File, Change hardware settings ,Delete a resource.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Tenant virtual environments are non-operable or operating in a degraded state due to an unapproved configuration change made to the IaaS infrastructure.
Basic Path:	BP1 – Well meaning cloud administrator makes a change to the environment without going through proper well thought out change control process. BP2 – Change has negative effect on devices supporting tenant virtual environments.
Alternate Paths:	AP1 - In task 1, rogue cloud administrator makes an unapproved change to the environment. AP2 - Change has negative effect on devices supporting tenant virtual environments
Mitigation Path	MP1 – in action 1 IaaS Security grant user rights included in the IDM Services and Auditing mitigate the changes administrators can make by enforcing separation of duties through the user rights and logging access attempts. MP2 – in action 2, IaaS Security IDM Services and Auditing

	mitigates by tracking what settings may have been changed to be a detective control during incident response.

Table 20: Perform unapproved change

Scenario:	Change hardware settings
Triggering event:	Cloud Administrator makes an approved configuration change to hardware settings on an IaaS device. These changes negatively impact the tenant environment.
Actors:	Cloud Administrator
Related misuse cases:	DDos Attack, Tap Tenant Data, Copy Tenant Virtual Machine Disk File, Perform unapproved change, Delete a resource.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Tenant virtual environments are non-operable or operating in a degraded state due to a hardware setting change made to the IaaS infrastructure.
Basic Path:	BP1 –cloud administrator makes an approved change to the hardware settings of a piece of equipment in the IaaS environment. BP2 – Change has negative effect on devices supporting tenant virtual environments.
Alternate Paths:	No alternate path
Mitigation Path	MP1 – in action 1 IaaS Security grant user rights included in the IDM Services and Auditing mitigate the changes administrators can make and

	limit the changes allowed that could possibly have ill effects on the client environment. . MP2 – in action 2, IaaS Security IDM Services and Auditing mitigates by tracking what settings may have been changed to be a detective control during incident response.

Table 21: Change hardware settings

Scenario:	Delete a resource.
Triggering event:	Rogue Cloud Administrator or unintended administrative activity deletes a resource in the environment the negatively affects a tenant virtual environment.
Actors:	Rogue Cloud Administrator, Unintended Administrative Activity
Related misuse cases:	DDos Attack, Tap Tenant Data, Copy Tenant Virtual Machine Disk File, Perform unapproved change, Change hardware settings.
Stakeholders:	All Subscribers of the IaaS C loud, Cloud administrative staff, IaaS Cloud owning company, Owners of data that resides in the cloud.
Pre-condition:	No Precondition
Post-condition:	Tenant virtual environment is negatively affected by the deletion of a resource in the IaaS environment.
Basic Path:	BP1 – Cloud Administrators have rights to delete some resources in the IaaS Cloud. BP2 – Rogue Cloud Administrator abuses access rights and deletes a resource in the IaaS Cloud. BP3 – Services that provide resources to the tenant virtual environment are affected. BP4 – Tenant loses virtual machines in their environment.
Alternate Paths:	AP1 – in action 1 Cloud Administrator accidentally deletes a resource in the IaaS Cloud. AP2 – Services that provide resources to the tenant virtual environment are affected. AP3 – Tenant loses virtual machines in their environment.

Mitigation Path	MP1 – in action 1 IaaS Security grant user rights included in the IDM Services and Auditing mitigate the deletions administrators can make and limit the deletions allowed that could possibly have ill effects on the client environment. . MP2 – in action 2, IaaS Security IDM Services and Auditing mitigates by tracking what resources may have been deleted to be a detective control during incident response and restore process.

Table 22: Delete a resource

The scenario that was run in the prototype environment for this use case was an attempt by a disgruntled cloud admin to copy data from a tenant's virtual machine, thus constituting a data leak. No special tools are required for this attack, just an abuse of administrative privileges is needed.

Intentional or unintentional data leak has occurred from tenant environment: A cloud administrator has used their administrative user account to copy a file off. - Procedure

1. Administrator launches WinSCP client from workstation.

2. Administrator connects to management console that manages the customer virtual machines

(esxi3.prod.com - 10.10.4.33) with WinSCP.

3. Administrator copies the file "Cust_1002.vmx" from a storage volume on esxi3.prod.com to

the local hard drive on the laptop.

4. Administrator disconnects from esxi3.prod.com and closes WinSCP.

4 Results and Analysis

4.1 Active Directory Implementation Issues and Solutions in the Prototype

VMware uses a component called Likewise to integrate with Active Directory. Likewise is a software agent that connects Linux, Unix and Mac OS X computers to Active Directory and authenticates users with their domain credentials [72]. If the Open Likewise administration guide is followed to implement the product in a Linux environment, Likewise supports the domain structure recommended in this thesis where a parent child trust exists. The chart below which is an excerpt from the Likewise administrative guide demonstrates that parent child trust relationships are supported:

Trust Type	Transitivity	Direction	Likewise Default Cell Support	Likewise Non-Default Cell Support (Named Cells)
Parent and child	Transitive	Two-way	Yes	Yes
External	Nontransitive	One-way	No	Yes
External	Nontransitive	Two-way	No	Yes
Forest	Transitive	One-way	No	Yes
Forest	Transitive	Two-way	Yes: Must enable default cell in both forests.	Yes

Table 23: Likewise – supported trust relationships

It was discovered while working with ESXi version 4.1 in the prototype environment that a bug is present in VMware's implementation of the Likewise agents. The symptom of the issue is that when an Active Directory user account is used to authenticate to an ESXi host and if it is a member of too many Active Directory groups, or nested in groups across an Active Directory trust, the user is not authenticated and an error of "Bad username or password" is returned to the user.

When presented with these issues VMware's support procedures were followed to enable logging for the Likewise agents. The daemon logs that are monitored for troubleshooting these issues are netlogond, which is used to join the domain, lwiod which is an SMB client driver, and lsassd which allows one to select the domain where users reside [73]. Enabling these logs demonstrated the root of the problem. Active Directory user accounts have a property called a Security Identifier (SID) which is a unique, immutable identifier of a user, user group or other security principal [74]. Windows grants or denies access and rights to resources based on access control lists which use SIDs to identify user accounts and their group memberships. When a user account is a member of a group, the group's SID is appended to the user account SID. The SID of each group that the user is a member of is appended to the user's SID. This SID can grow quite large when a user account is a member of nested groups across a domain trust. VMware's implementation of the Likewise agent is limited in the length of the SID that it can resolve. So, if the user is a local domain user who is only a member of minimal Active Directory groups, the user can log into the ESXi host without issue. The problem arises when the user is from another domain The SID that the Likewise agents have to resolve is too long and the login fails. As Stated earlier, VMware is now aware of the problem, but a patch was not available to solve the issue in the prototype. Further research has indicated that Xen hypervisors would not have this issue but time did not allow testing of the Xen hypervisor in this prototype. To work around this issue for demonstration purposes, an organizational unit was created in the prod.com domain to hold the Active Directory users and groups that would be used for subscriber accounts.

Vmware is currently working on the issue. The only answer VMware has provided is that they are including the fix in future releases of ESXi and have not yet finished developing a patch for existing versions of ESXi.

4.2 Misuse Case #1

Scenario Chosen: Denial of Service Attack on the portal (DoS Attack)

4.2.1. Results

Raw Event	month	day	hour	minute	second	weekday	year	date_zone	error	local	peer
74D2DB90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35388, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35388	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.064 74DF0B90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35384, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35384	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.064 73DC2B90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35387, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35387	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.062 74AE4B90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35385, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35385	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.061 74EF4B90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35381, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35381	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.061 74BE8B90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35383, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35383	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.060 73D81B90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35386, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35386	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.060 74CABB90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35382, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35382	10.10.4.33:443
Mar 4 15:41:54 10.10.4.33 Mar 4 20:42:29 Hostd: [2012-03-04 20:42:29.056 74DAFB90 warning 'Proxysvc'] SSL Handshake failed for stream TCP(local=10.10.4.35:35380, peer=10.10.4.33:443), error=SSL Exception: BIO Error	march	4	15	41	54	sunday	2012	local	SSL	10.10.4.35:35380	10.10.4.33:443

Table 24: Misuse case #1 log file results

The log results displayed above were extracted from the centralized logging server of the prototype cloud. These entries are a sampling of the detected activities during the denial of service attack that was launched. There were over 800 log events related to the attack. The log entries are a repeat of what is displayed above.

The source of these logs entries are events from the hostd log maintained on the ESXi server where the customer virtual servers reside. The query used to gather these log entries was a search of any event that was recorded that included the ESXi server's IP address (10.10.4.33) during the space of time when the attack was taking place. The only entries that were returned by the search were these events reported by the hostd process via syslog. The source of the attack was on the same subnet, so no firewalls were involved to report any data and there were no errors

that occurred at the switching layer to be reported.

4.2.2 Analysis

The VMware hostd service is responsible for managing most of the operations on an ESXi server. Since this DoS attack was targeted against the ESXi web portal of this server, the hostd logs were where the errors were reported.

The raw event contains any warning or error conditions that occurred. The time of the event as well as the local and any peer IP address and port involved with the event are also reported. The event logs displayed above show that the Proxy service is reporting continual SSL Handshake failures on source port 443, which is the port that SSL communicates on. These failures correlate to the exact time the DoS attack was launched against the SSL service of this ESXi server.

When this particular network based attack was launched from a subscriber's virtual machine, it can be determined where the attack is coming from and when the attack has been launched, but it cannot be determined who is causing the attack in this environment. This is due to the fact that when the attack was launched, the ESXi management console was not used to log on to the rogue host. An SSH client was used and connected to the rogue host directly. A direct log on to a subscriber's host is outside the scope of an IaaS cloud infrastructure's identity management and auditing systems. This activity would only be monitored by a subscriber's auditing systems. The provider is ultimately responsible for the infrastructure of the cloud, but as this example demonstrates, there needs to be a partnership with the subscribers. Minimally, there needs to be a terms of usage agreement with the subscribers and a service level agreement with the IaaS cloud provider. These agreements would help develop trust between the cloud provider and the subscriber. The rules of behavior that would need to be agreed upon would be a responsibility of who would monitor the subscriber's internal network so attacks like this could be detected or avoided.

4.3 Misuse Case #2

Scenario Chosen: Copy a co-tenant's virtual machine

4.3.1 Results

Raw Event	month	day	hour	minute	second	weekday	year	date_zon	local	peer
Mar 4 13:47:07 10.10.4.33 Mar 4 18:47:41 Hostd: [2012-03-04 18:47:41.680 72CCBB90 verbose 'Cimsvc'] Ticket issued for CIMOM version 1.0, user root	march	4	13	47	7	sunday	2012	local		
Mar 4 13:47:02 10.10.4.33 Mar 4 18:47:36 Hostd: [2012-03-04 18:47:36.452 72C40B90 verbose 'Proxysvc Req00404'] New proxy client TCP(local=10.10.4.5:4857, peer=10.10.4.33:80)	march	4	13	47	2	sunday	2012	local	10.10.4.5:4857	10.10.4.33:80
Mar 4 13:47:02 10.10.4.33 Mar 4 18:47:36 Hostd: [2012-03-04 18:47:36.450 FFFBAE90 verbose 'Vmsvc'] RefreshVms updated overhead for 1 VM	march	4	13	47	2	sunday	2012	local		
Mar 4 13:47:02 10.10.4.33 Mar 4 18:47:36 Hostd: [2012-03-04 18:47:36.449 FFFBAE90 verbose 'vm:/vmfs/volumes/4f40f1e1-e30094c8-f655-001438bf16d8/backtrack_Cust_1001/backtrack_Cust_1001.vmx'] Actual VM overhead: 139194368 bytes	march	4	13	47	2	sunday	2012	local		
Mar 4 13:46:46 10.10.4.33 Mar 4 18:47:20 Hostd: [2012-03-04 18:47:20.993 72A40B90 warning 'UserDirectory'] Group lookup failed for 'PROD\ESX Admins'	march	4	13	46	46	sunday	2012	local		
Mar 4 13:46:46 10.10.4.33 Mar 4 18:47:20 nssquery: Group lookup failed for 'PROD\ESX Admins'	march	4	13	46	46	sunday	2012	local		
Mar 4 13:46:02 10.10.4.33 Mar 4 18:46:36 Hostd: [2012-03-04 18:46:36.446 728E7B90 verbose 'Vmsvc'] RefreshVms updated overhead for 1 VM	march	4	13	46	2	sunday	2012	local		
Mar 4 13:46:02 10.10.4.33 Mar 4 18:46:36 Hostd: [2012-03-04 18:46:36.445 728E7B90 verbose 'vm:/vmfs/volumes/4f40f1e1-e30094c8-f655-001438bf16d8/Cust_1002/Cust_1002.vmx'] Actual VM overhead: 98099200 bytes	march	4	13	46	2	sunday	2012	local		
Mar 4 13:45:46 10.10.4.33 Mar 4 18:46:20 Hostd: [2012-03-04 18:46:20.662 FFFBAE90 warning 'UserDirectory'] Group lookup failed for 'PROD\ESX Admins'	march	4	13	45	46	sunday	2012	local		
Mar 4 13:45:46 10.10.4.33 Mar 4 18:46:20 nssquery: Group lookup failed for 'PROD\ESX Admins'	march	4	13	45	46	sunday	2012	local		
Mar 4 13:45:36 10.10.4.33 Mar 4 18:46:11 Hostd: [2012-03-04 18:46:11.142 73D81B90 verbose 'Cimsvc'] Ticket issued for CIMOM version 1.0, user root	march	4	13	45	36	sunday	2012	local		
Mar 4 13:45:05 10.10.4.33 Mar 4 18:45:39 Hostd: [2012-03-04 18:45:39.923 728E7B90 info 'TaskManager' opID=D641F011-0000020F] Task Completed : haTask-ha-host-vim.option.OptionManager.updateValues-506 Status success	march	4	13	45	5	sunday	2012	local		
Mar 4 13:45:05 10.10.4.33 Mar 4 18:45:39 Hostd: [2012-03-04 18:45:39.916 728E7B90 info 'SyslogConfigProvider' opID=D641F011-0000020F] Set called with key 'Syslog.Remote.Port' value '515'	march	4	13	45	5	sunday	2012	local		

Table 25: Misuse case #2 log file results

The source of these log entries are events from the hostd log maintained on the ESXi server where the customer virtual servers reside. The query used to gather these log entries was a search of any event that was recorded that included the ESXi server's IP address (10.10.4.33) during the space of time when the attack was taking place. The only entries that were returned by the search were these events reported by the hostd process via syslog. The source of the attack was on the same subnet, so no firewalls were involved to report any data and there were no errors that occurred at the switching layer to be reported. The time related entries in the sample logs above are self explanatory.

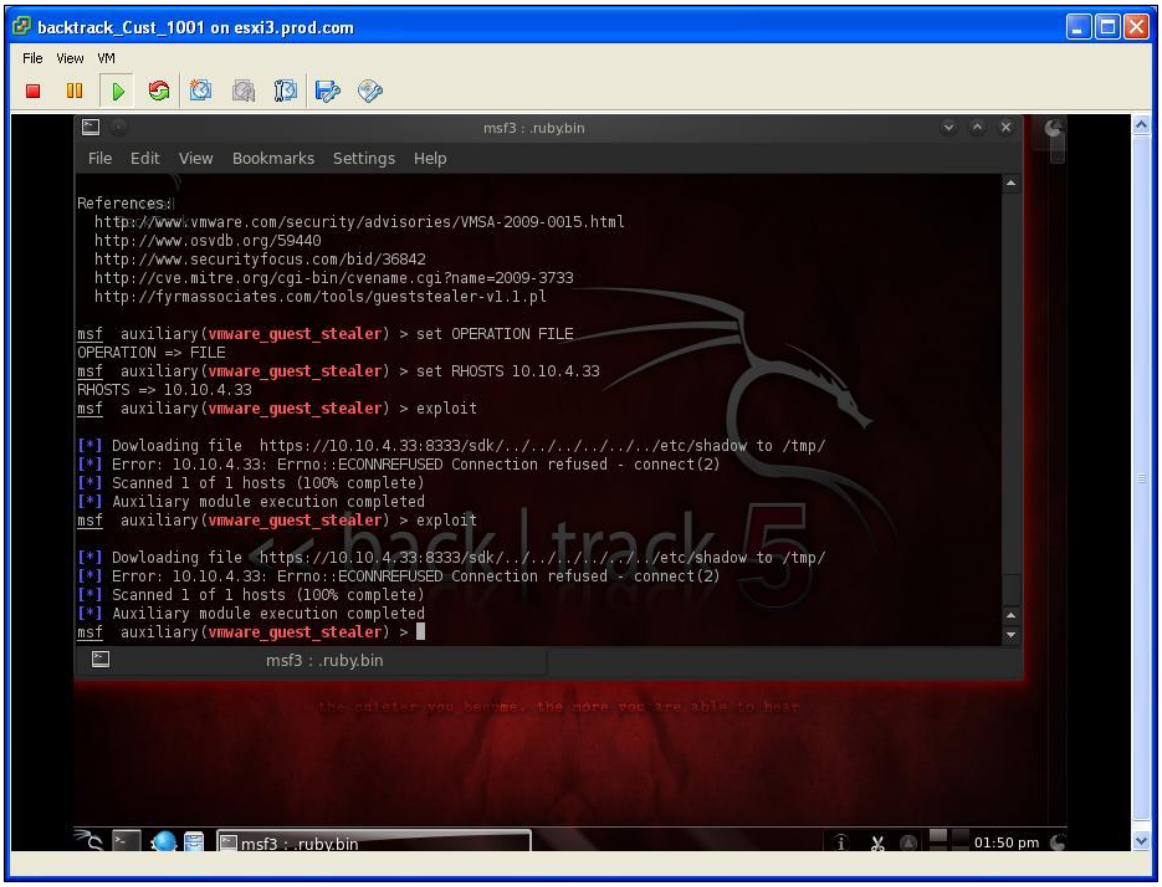

Figure 8: Attacking with vmware_guest_stealer

4.3.2 Analysis

When examining the raw events, nothing is seen that directly indicates an attack was attempted, however there are a few interesting things to note. One can see the failed group lookups for “PROD\ESX_Admins”. This lookup issue occurred due to the issue that was discussed about the implementation of the Likewise agents having a bug. The logs also indicate the presence of a virtual machine with a VMX file named “backtrack_Cust_1001.vmx” A VMX file is the primary configuration file for a virtual machine on a ESXi host. For those not familiar with penetration testing and hacking, BackTrack is the name of a very well known Linux build based on Ubuntu that contains many software utilities which are used for hacking. This is a clear

indication that there may be a rogue virtual machine present in the environment and at very least warrants further investigation by the security team of the IaaS cloud. The logs at 13:45:05 show when the administrator logged into the ESXi server as root and configured the ESXi server to send its syslog messages to destination port 515. This was a maintenance task that was performed before simulating the attack to make sure any events that the hostd service recorded would get sent using syslog to the central log server on the network. With the exception of the log files that reported that the backtrack_Cust_1001.vmx file was on a local storage volume at 13:47:02, none of the logs captured are remotely related to the attack that failed.

This simulation with vmware_guest_stealer demonstrated another instance where the limitation is that this rogue host is present within a subscriber's environment. This is outside the scope of the IaaS Cloud's identity management and logging mechanisms. This failed attack cannot be traced to an actual user account relying only on the cloud's auditing mechanisms. The creation of the rogue virtual machine could be traced to a user. The powering on of the virtual machine can also be traced to a user account, because a user account in the sub.com or prod.com domain is needed in order to perform either of those actions. The attack itself cannot be determined by examining the logs during the time of the attack. This can be seen by viewing the logs above that were taken from the victim ESXi host.

Even with Identity Management and Auditing being in place, the nefarious activity was not captured in the centralized audit logs. Other security controls that were in place blocked the success of this attack. In this case, current security patches on the ESXi hypervisor stopped this attack. The vmware_guest_stealer module tries to take advantage of an old vulnerability that allows the unauthenticated traversal of ESXi's storage volumes to browse then download a virtual machine file. None of the log entries that were recorded are related to the attack that took place. Fortunately, the security patch did its job. Under normal circumstances, this failed attack would have gone unnoticed. This is another example of where a trusted relationship with the subscriber

is essential. Monitoring and logging within the subscriber's virtual container would most likely have captured this attack attempt. This also shows that logging capabilities are highly dependent upon the capabilities of the operating system on the host. ESXi did not report the event, so it never showed up in the centralized logs. The only activity that was captured was the logon of root to the ESXi host from 10.10.4.5 after the fact to verify the status of the systems and logs after the simulation of the misuse case. Future research could examine how centralized logging mechanisms of an IaaS cloud could capture and report on these types of failed attempts. Perhaps, these activities could be captured with internal IPS devices and custom written signatures. Then those alerts could be forwarded via syslog to the central logging server.

In the prototype, multiple attempts were tried to make this attack a success. The oldest version of the ESXi software available to test with was ESXi 3.5, and the attack simulation was as unsuccessful against that version as it was against the 4.1 version. Attacks on the ESXi 3.5 hypervisor provided no log evidence of the attack attempt either. The only VASTO module that was successful was a fingerprinting module named vmware_version.rb. The test of this module, although successful, as it was able to correctly identify a number of details about the hypervisor, still did not leave any evidence of a successful attack in the audit logs of the IaaS cloud prototype. These trials indicate that even if the vmaware_guest_stealer module had been successful in this prototype, the likely outcome would be that no indication of the attack would be captured by the hypervisor logging, thus leaving the attack undetected. The only device logs that would have captured any activity would be an intelligent storage device that could be configure to record I/O activity on the storage volume.

4.4 Misuse Case #3

Scenario Chosen: Change infrastructure settings

4.4.1 Results

Raw Event	month	day	hour	minute	second	weekday	year	date_zone	user
Power Off virtual machine Cust_1002 Completed PROD\vmadmin1 3/4/2012 17:18 3/4/2012 17:18 3/4/2012 17:18	march	3	4	17	18	sunday	2012	local	prod\vmadmin1
Mar 4 17:17:09 10.10.4.33 Mar 4 22:17:43 Hostd: [2012-03-04 22:17:43.657 281C5B90 info 'ha-eventmgr' opID=9F0644FF-00000003] Event 42 : User PROD\vmadmin1@10.10.4.5 logged in	march	3	4	17	9	sunday	2012	local	
Mar 4 17:17:09 10.10.4.33 Mar 4 22:17:43 Hostd: [2012-03-04 22:17:43.656 281C5B90 info 'Vimsvc' opID=9F0644FF-00000003] [Auth]: User PROD\vmadmin1	march	3	4	17	9	sunday	2012	local	
Mar 4 17:17:09 10.10.4.33 Mar 4 22:17:43 Hostd: Accepted password for user PROD\vmadmin1 from 10.10.4.5	march	3	4	17	9	sunday	2012	local	
Mar 4 17:17:09 10.10.4.33 Mar 4 22:17:43 Hostd: pam_per_user: create_subrequest_handle(): doing map lookup for user "prod\vmadmin1"	march	3	4	17	9	sunday	2012	local	
Mar 4 17:17:09 10.10.4.33 Mar 4 22:17:43 Hostd: pam_per_user: create_subrequest_handle(): creating new subrequest (user="prod\vmadmin1", service="system-auth-generic")	march	3	4	17	9	sunday	2012	local	prod\vmadmin1
Mar 4 17:17:09 10.10.4.33 Mar 4 22:17:43 Hostd: pam_per_user: create_subrequest_handle(): doing map lookup for user "prod\vmadmin1"	march	3	4	17	9	sunday	2012	local	
Mar 4 17:16:45 10.10.4.33 Mar 4 22:17:19 Hostd: "vmadmin1"	march	3	4	16	45	sunday	2012	local	
Mar 4 17:16:45 10.10.4.33 Mar 4 22:17:19 Hostd: Rejected password for user vmadmin1 from 10.10.4.5	march	3	4	16	45	sunday	2012	local	
Mar 4 17:16:45 10.10.4.33 Mar 4 22:17:19 Hostd: [2012-03-04 22:17:19.467 28340B90 info 'ha-eventmgr' opID=D36FACD0-00000003] Event 41 : Cannot login vmadmin1@10.10.4.5	march	3	4	16	45	sunday	2012	local	
Mar 4 17:16:43 10.10.4.33 Mar 4 22:17:17 Hostd: pam_per_user: create_subrequest_handle(): creating new subrequest (user="vmadmin1", service="system-auth-generic")	march	3	17	16	43	sunday	2012	local	vmadmin1
Mar 4 17:16:43 10.10.4.33 Mar 4 22:17:17 Hostd: pam_per_user: create_subrequest_handle(): doing map lookup for user "vmadmin1"	march	3	17	16	43	sunday	2012	local	

Table 26: Misuse case #3 log file results

The source of these logs entries are events from the hostd log and the “events and alerts” log maintained on the ESXi server where the customer virtual machines reside. The query used to

gather these log entries was a search of any event that was recorded that included the ESXi server's IP address (10.10.4.33) during the space of time when the attack was taking place. The time related entries are self explanatory. The raw events from the hostd log activities have been explained in prior sections. The events and alerts log lists event details from commands that have been launched using the VMware client to connect to the management IP address of an ESXi server. The first log entry above showing the power off virtual machine activity at 17:18 is from the events and alerts log. The hostd log entries can be distinguished from the events and alerts log by the fact that "Hostd:" is included in all raw event fields after the time stamp.

4.4.2 Analysis

When demonstrating this misuse case, the log entry from hostd clearly shows when the subscriber administrator logged into the ESXi host:

Mar 4 17:17:09 10.10.4.33 Mar 4 22:17:43 Hostd: pam_per_user: create_subrequest_handle(): creating new subrequest (user="prod\vmadmin1", service="system-auth-generic") march 3 4 17 9 sunday 2012 local prod\vmadmin1

The log entry from the events and alerts log what activity was performed while logged into the ESXi server with the VMware client:

Power Off virtual machine Cust_1002 Completed PROD\vmadmin1 3/4/2012 17:18 3/4/2012 17:18 3/4/2012 17:18 march 3 4 17 18 sunday 2012 local prod\vmadmin1

This is a clear cut example of when the IaaS Cloud identity management and auditing is useful as a security tool in and of itself. When a device that is part of the cloud infrastructure is used to perform an activity by a defined user account, the complete transaction with all of its details can be directly observed. Most identity management and logging systems are not implemented in such a way where this condition is maximized. The goal of the ten primary recommendations which are presented in this thesis is to maximize the conditions where complete transactions can be observed and tied to a user account for auditing.

The nature of an IaaS cloud competes with this goal. Part of the trust that needs to be maintained in an IaaS cloud is that the provider will not view or operate on subscriber data within their virtual container. This will restrict any auditing or logging data in the customer environment from the subscriber. Without this data, it will always be difficult to observe all activity affecting the cloud. This can be mitigated by the service level agreements mentioned in the prior section. Some providers offer security monitoring services to cloud subscribers as a value added service. These additional services would be another mitigation, especially if log data from these services can be aggregated and some business intelligence and trending data can be extracted.

4.5 Misuse Case #4

Scenario Chosen: Intentional or unintentional data leak has occurred from the tenant environment.

4.5.1 Results

Raw Event	month	day	hour	minute	second	weekday	year	date_zone	user
Mar 4 20:00:15 10.10.4.33 Mar 5 01:00:49 dropbear[30240]: exit after auth (PROD\vmadmin1): Exited normally	march	4	20	0	15	sunday	2012	local	
Mar 4 19:59:00 10.10.4.33 Mar 5 00:59:34 dropbear[30240]: PAM password auth succeeded for 'PROD\vmadmin1' from 10.10.4.5:2265	march	4	19	59	0	sunday	2012	local	
Mar 4 19:59:00 10.10.4.33 Mar 5 00:59:34 dropbear[30240]: pam_per_user: create_subrequest_handle(): creating new subrequest (user="PROD\vmadmin1", service="system-auth-generic")	march	4	19	59	0	sunday	2012	local	PROD\vmadmin1
Mar 4 19:59:00 10.10.4.33 Mar 5 00:59:34 dropbear[30240]: pam_per_user: create_subrequest_handle(): doing map lookup for user "PROD\vmadmin1"	march	4	19	59	0	sunday	2012	local	

Table 27: Misuse case #4 log file results

The source of the logs captured in this instance is from the dropbear service. Dropbear is the service that handles SSL connections to the server. Locally the dropbear service logs to the local location of /var/log/secure. The ESXi server in the prototype is configured to send all of its logging to the centralized log server using syslog. No log files were present from the file system,

which is unfortunate, because those may have shown what file operations occurred while connected to the ESXi server.

4.5.2 Analysis

When using administrative rights to copy a file from the hypervisor, the basic hypervisor logging, identity management and central logging is not enough to indicate what type of breach has occurred. The dropbear logs show that a connection was made using the SSH service as well as the username that requested the SSH service. This prototype solution was able to track down who made a breach, but that only would have been discovered through an audit after the fact, verifying administrative logins. What would be more helpful is if the actual SSH connection and file copy operations were captured in log files. This was not possible within this prototype because, even with the ESXi logging level set to verbose, then next trivia, the only operations that were captured was the authentication. Ideally, the storage volumes containing virtual machine files should be stored on a storage area network that provides the logging capabilities needed to capture file operations. If this logging feature was available, the correlation of the administrative login, to the file operations would have been trivial with the logging solution that is used in the prototype.

4.6 General Analysis Observations

Attacks coming from rogue virtual machines from within subscribers' virtual containers are detectable; however, additional information about the environment is needed to tie a source user to the attack. One can examine the attack source and if subscriber mappings to IP address space is maintained a correlation is possible. The information can be used to correlate an attack time through the identity management system to a user or group of users that are operating within the subscribers’ network space at that time. This is why it is important not to use shared accounts for any subscribers that can be logged into the system. This correlation to user account fails is

when the subscriber's virtual container is extended back to the subscriber's on premises network through a site to site VPN. The creator of the rogue virtual machine can be determined, but the person logged on and launching the attack might not be without the assistance of the subscriber's own monitoring mechanisms. The virtual machine creator is detectible due to the centralized auditing which has been suggested should be in conjunction with an identity management solution. Denial of Service attacks can't be prevented with identity management, but the auditing function allows the administrators to discover the source of the DoS and take proper measures. Events from IaaS infrastructure hosts and devices can provide audit logs to investigate internal DoS events and events from edge IDS devices can provide logs to investigate external DoS events. These misuse cases demonstrated that identity management and central logging is not a silver bullet to the cloud’s security worries. However, it is an essential component to be included with multiple other security controls. Logging is dependent on software from firmware, operating systems and applications properly reporting events.

5. Discussion

The recommendations presented in this thesis were not devised through testing in the prototype environment. They were developed from technical experiences working at an IaaS cloud datacenter and through the background research that was performed on the topic of identity management in the cloud. The misuse cases tested earlier were meant to demonstrate what mitigations an identity management and auditing solution configured as described in section 3 of this thesis could provide an IaaS cloud. With the exception of the described bug discovered with ESXi and its Likewise components, all recommendations which have been presented were configured in the prototype. None of the tests failed due to a misconfiguration of the identity management implementation. The failures to mitigate attacks were because the infrastructure components themselves did not have the capability to log the event, or the attack was simply outside the scope of the identity management solution that was implemented in the IaaS infrastructure. This was particularly the case when something was occurring within the subscriber virtual environments where the provider had no visibility.

The RBAC model is a necessity to be used for security administration in the IaaS Cloud. This recommendation was made because RBAC is a popular security model that is implemented in most technologies that comprise an IaaS cloud. Microsoft Active Directory supports it and RBAC is a model that can scale with an IaaS cloud infrastructure.

Two separate domains should be used for identity management. One domain for the IaaS provider and one for the user accounts of all of the subscribers. These domains should be in a parent child trust relationship with the IaaS provider administrative accounts being in the parent domain. The user accounts provided for subscribers to manage their virtual environments reside in the child domain. A trust relationship exists between the two domains where the parent domain trusts the child domain and allows access to the hypervisor host computers which are contained in the parent domain. The subscriber's user accounts should be organized such that only those that

belong to the same subscriber company are grouped together. An organizational unit can be used for each subscriber to allow security account policies that can be applied to the user accounts. These policies would govern properties like password complexity, lockout and reset policies. This recommendation of using a separate domain for subscriber and provider administrative accounts introduces an additional level of security. This additional level of security allows for additional granularity in the assignment of user account and group access rights. In multi-tenant environments like a public IaaS cloud, the ability to be more granular in the assigning of access rights is a benefit.

Due to use of pre-built virtual machines and automated deployment mechanisms available to subscribers, customized virtual machine and network container administrative accounts need to be guaranteed unique and complex for each and every individual subscriber. This precaution is important so that someone cannot use the known administrative credentials of a pre-created virtual machine to obtain access to any other subscriber's virtual machine. This stresses the importance of a secure automated deployment process.

Centralized logging and auditing of all system and user activity is critical in deterring insider threats and creating trust in the cloud. Auditing needs to occur for the infrastructure itself and for the components in subscriber environments. A centralized identity management solution is essential for successful logging and auditing. This solution is not complete without the cooperation of the cloud subscribers. The misuse cases showed that the IaaS cloud central auditing systems are generally blind to activities within each subscriber's virtual containers. Current measures to mitigate this gap are service level agreements that define what types of virtual resources can be deployed within the cloud. These agreements can also add monitoring capabilities to the subscriber's responsibilities. Other IaaS providers offer monitoring and security services to subscribers as an additional service. This additional monitoring can capture events occurring within a subscriber's virtual container.

Time must be synchronized across the entire environment. This observation was made early in the research for this thesis. Any slips at all can cause correlation failures when auditing across multiple systems. Virtualization Management tools need better integration into the roles and permissions of the underlying hypervisor management servers such as VMware vCenter. Most management tools have elevated access to the IaaS cloud environment. As demonstrated by the Active Directory integration issues which were discovered with Vmware ESXi, it is still difficult to configure these management tools to leverage identity management solutions. These gaps may allow an administrator to gain more access rights into the environment than are required for their job function. This is a vulnerability that needs additional attention.

Capabilities offered by cloud providers are not currently adequate to meet enterprise requirements. Subscribers should avoid proprietary solutions such as creating custom connectors unique to cloud providers, as these exacerbate management complexity. These custom connections also make it more difficult to migrate data out of the cloud if a subscriber wishes to move to another provider. Subscribers should leverage standard connectors provided by cloud providers. If a cloud provider does not currently offer standards based connectors, the subscriber should request them or look to another provider.

Cloud subscribers should modify or extend their authoritative repositories of identity data so that it encompasses applications and processes in the cloud. Both the cloud provider and the customer enterprises should consider the challenges associated with credential management and strong authentication, and implement cost effective solutions that reduce the risk appropriately.

IaaS, authentication strategies can leverage existing enterprise capabilities. For IT personnel, establishing a dedicated VPN will the best option. By leveraging existing systems and processes that are already present in most enterprises, subscribers will be able to extend their current identity management solution into the cloud without much additional complexity and

expense. A possible solution is creating a dedicated VPN tunnel to the subscriber's corporate network or federation. A dedicated VPN tunnel works better when the application leverages existing identity management systems. It is best when identity data comes from a subscribers existing authoritative source such as a Single Sign On solution or LDAP based authentication. In cases where a dedicated VPN tunnel is not feasible, applications should be designed to accept authentication assertions in various formats (SAML, WS-Federation, etc), in combination with standard network encryption such as SSL. This approach enables the subscriber's organization to deploy federated SSO not only within an enterprise, but also to cloud applications.

In order to enable strong authentication (regardless of technology), cloud applications should support the capability to delegate authentication to the subscriber that is consuming the services, such as through SAML. Cloud providers should consider supporting various strong authentication options such as One-Time Passwords, biometrics, digital certificates, and Kerberos. This will provide another option for subscribers to use their existing infrastructure.

In a Cloud Computing environment, federation of identity is key for enabling allied enterprises to authenticate, provide single or reduced Sign-On (SSO), and exchange identity attributes between the service provider and the identity provider. Organizations considering federated identity management in the cloud should understand the various challenges and possible solutions to address them with respect to identity lifecycle management, authentication methods, token formats, and non-repudiation.

Enterprises looking for a cloud provider should verify that the provider supports at least one of the prominent standards (SAML and WS-Federation). SAML is emerging as a widely supported federation standard. Support for multiple standards enables a greater degree of flexibility. Cloud providers should have flexibility to accept standard federation formats from different identity providers. However most IaaS cloud providers support only a single standard.

Cloud providers desiring to support multiple federation token formats should consider implementing some type of federation gateway.

Organizations may wish to evaluate Federated Public SSO versus Federated Private SSO. Federated Public SSO is based on standards such as SAML and WS-Federation with the cloud provider, while Federated Private SSO leverages the existing SSO architecture over VPN. In the long run Federated Public SSO will be ideal; however an organization with a mature SSO architecture and limited number of cloud deployments may gain short-term cost benefits with a Federated Private SSO.

Identity management is a crucial component of the public IaaS cloud. The application of identity management in the cloud is still in its infancy and continued research is required. The function of audit in the cloud is closely tied to identity management. Further, in order for companies to move their data and applications to the cloud, a level of trust must be attained. This level of trust has not yet been demonstrated in current deployments. Auditing functions which are tied to identity management are highly dependent on the log sources provided by various operating systems and firmware. Another area of future research would be to study improvements that could be made with the logging functions of operating systems, firmware and applications to support better auditing in the cloud. Improving the efficiency of transporting log file data across the network is another area that needs additional research.

Research regarding the extending of subscribers' existing identity management into the cloud is crucial to establishing trust in the cloud. Experiences from employment as a security engineer in a cloud data center has demonstrated that most of the data being moved to the cloud are pilot programs, and tertiary applications that do not store critical information such as email and portal applications. The cloud is beginning to be used as a data backup and a fail-over-site target. No one is currently moving their critical company data on to the cloud. This is due to a lack of trust in the cloud and a loss of control over data once it is in the cloud. Cloud providers

must move away from the proprietary interfaces that are being used today. These interfaces lead to “data lock in” that prevents subscribers from easily migrating their data if they choose to move to another provider.

The analysis in this thesis showed that many issues still remain in the public IaaS cloud that keeps it from being trusted by many prospective subscribers to house their critical data. A properly implemented identity management solution addresses many of these issues. The best practices recommended in this thesis position identity management as an additional set of controls for an IaaS provider to use to secure the infrastructure of the cloud. Active Directory was used as the identity management solution in the prototype because it is one of the most used directory service. It supports the RBAC security model which was recommended because of its scalability and ease of managing access rights. As the cloud infrastructure grows with more subscribers, new roles will be created and can be mapped to security groups for each newly subscribing company. The proper management of access rights a rapidly growing IaaS cloud is crucial to establishing trust. The use of two Active Directory domains, one for the provider’s resources and accounts and one for the subscriber’s accounts provides additional security to the identity management solution. A network layer separation was also recommended as a best practice. The management traffic that flows across an IaaS infrastructure should be isolated from any of the subscriber networks. This isolation also applies to identity management traffic. This isolation helps protect from tampering with identity traffic.

There are still many concerns remaining with the common use of pre-built virtual machine and automated deployment mechanisms in the IaaS cloud. One of the primary tenants of the cloud is increased efficiency. Pre-built virtual machines cut server deployment times down to minutes instead of hours. Pre-built virtual machines work great in a private cloud. Using them in a public cloud introduces additional risks. These pre-built virtual machines are typically deployed with the same local administrator credentials if precautions are not taken. The recommendation to

employ scripted deployments of these pre-built virtual machines was made to address this issue. The various guest operating systems that are virtualized in the cloud provide APIs that can be used by deployment scripts to randomize, or let subscribers choose their own local passwords to be used. Without these precautions, pre-built virtual machines could present an identity management nightmare in a public cloud. All subscriber virtual machines would use the same local administrator credentials. If the subscriber doesn't immediately change the administrator password upon deployment, anyone familiar with the environment could have full administrative access to the virtual machine.

Until these problems are solved, the hype over the public cloud will remain just that. There are a lot of potential efficiency gains available with the public IaaS cloud. Improvement is being made in these research areas every day. As the development of identity management technologies continue, this paradigm shift to public cloud computing will deliver on all of its promises.

5.1 Future Work

There were many misuse case scenarios that were presented in this thesis that were not simulated in the prototype due to the limited scope of the lab environment. These misuse cases need to be simulated and investigated to determine what role identity management plays in the mitigation of those attacks. Issues with the cloud control portal need to be further investigated. Newer hardware was required to properly test a multi-tenant cloud control portal in the prototype environment. Fully integrating a software solution such as Eucalyptus would provide an ideal platform to test the integration of identity management into the cloud control portal component of the IaaS cloud. Further investigation into the logging capabilities and identity management integration capabilities with storage area networks is required. Storage is a core resource that is virtualized in the cloud. Researchers could examine storage related protocols such as iSCSI, fiber

channel and fiber channel over Ethernet to determine how to authenticate and authorize those protocols so that they don't become compromised. Study remains on the topic of live migrations. Outside of assuring that live migration traffic only transmits over an isolated network segment, researchers can study how the authentication and authorization practices of identity management could assist in protecting that communication.

Extending a subscriber's identity management into the cloud is an important piece to establishing trust in the cloud. A test of extending a subscriber's identity management into the prototype environment was not performed. The next step towards this goal is to extend the prototype to include an offsite subscriber. This would allow further testing with VPN tunnels and common protocols such as SAML and WS-Security to extend an identity management implementation into the cloud.

6. LIST OF REFERENCES

[1] “Security Guidance for Critical Areas of Focus in Cloud Computing v2.1”, Section III Operating in the Cloud – Domain 12: Identity and Access Management, pp. 63 – 67, Prepared by the Cloud Security Alliance, December 2009. Internet: https://cloudsecurityalliance.org/csaguide.pdf, [March 26, 2012]

[2-3] Mell, Peter, Grance Tim, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, September 2011, Internet: http://csrc.nist.gov/publications/nistpubs/800-145.pdf, [March 26, 2012]

[4] Popa, Yu, Ko, Ratnasamy, Stoica, October 2010 ‘CloudPolice: taking access control out of the network’ Hotnets ’10: Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks, pp. 1-6.

[5] Krieger, McGachey, Kanevsky, “Enabling a marketplace of clouds: VMware’s vCloud director”, ACM SIGOPS Operating Systems Review, Volume 44 Issue 4, December 2010, pp. 103-114.

[6] Bias, Randy “Amazon's EC2 Generating 220M+ Annually”, October 1, 2009, Internet: http://www.cloudscaling.com/blog/cloud-computing/amazons-ec2-generating-220m-annually/ [October 9, 2011]

[7] Amazon Web Services, Internet: http://aws.amazon.com , [October 9, 2011]

[8] Erickson, Heller, Yang, Chu, Ellithorpe, McKeown, Parulkar, Rosenblum, Whyte, Stuart, “Optimizing a Virtualized Data Center”, ACM Sigcomm 2011, Internet: http://conferences.sigcomm.org/sigcomm/2011/papers/sigcomm/p478.pdf [March 26, 2012]

[9] “Cisco Global Cloud Index: Forecast and Methodology, 2010 – 2015”, Cisco, 2011. Internet: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf

[10] Hommel, Wolfgang and Boursas, Latifa. “Policy-based Service Provisioning and dynamic Trust Management in Identity Federations”, IEEE International Conference on Communications 2006, June 2006

[11] Pfitzmann and Waidner, “Federated Identity-Management Protocols”, Security Protocols Lecture Notes in Computer Science, 2005, Volume 3364, Springer Berlin / Heidelberg, pp. 153-174.

[12] Josang, Fabre, Hay, Dalziel, Pope, “Trust Requirements in Identity Management”, ACSW Frontiers ’05 Proceedings of the 2005 Australasian workshop on Grid computing and e-research, Volume 44, Australian Compute Society, Inc., pp. 99-108.

[13] Rajkumar, Rajiv, Rodrigo, Ching-Hsien, Laurence, Jong, Sang-Soo, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", Algorithms and Architectures for Parallel Processing, Lecture Notes in Computer Science, 2010 Volume 6081, Springer Berlin / Heidelberg, pp. 13-31.

[14] Kundra, Vivek, U.S. Chief Information Officer, "Federal Cloud Computing Strategy", February 8, 2011., PowerPoint slides, Executive Office of the President of the United States, Internet: http://www.cio.gov/documents/Vivek-Kundra-Federal-Cloud-Computing-Strategy-02142011.pdf.

[15] Kundra, Vivek, U.S. Chief Information Officer, "Federal Cloud Computing Strategy", February 8, 2011, Executive Office of the President of the United States, Internet: http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf [March 28, 2012]

[16] Deloitte & Touche LLP, "Leveraging existing IAM systems in a cloud computing environment Overview", Deloitte Consulting's slide deck mentioned on the (ISC)2 Thinkt@nk roundtable from October 13th, 2010.

[17] "Security Guidance for Critical Areas of Focus in Cloud Computing v2.1", Section III Operating in the Cloud – Domain 12: Identity and Access Management, pp. 63 – 67, Prepared by the Cloud Security Alliance, December 2009. Internet: https://cloudsecurityalliance.org/csaguide.pdf, [March 26, 2012]

[18-19] Michael Armbrust, et al, Above the Clouds: A Berkeley View of Cloud Computing, EECS Department University of California, Berkeley Technical Report No. UCB/EECS-2009-28, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, Feb, 2009. Internet: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

[20] "SOAP Introduction", W3Schools, Internet: http://www.w3schools.com/soap/soap_intro.asp", [December 22, 2011]

[21] "SOAP Tutorial", W3Schools, Internet: http://www.w3schools.com/soap/default.asp", [December 22, 2011]

[22] Gaedke, Meinecke, Nussbaumer, "A Modeling Approach to Federated Identity and Access Management", WWW '05 Special interest tracks and posters of the 14th international conference on World Wide Web, 2005 ACM.

[23] "Web Service Security patterns – Community Technical Preveiw", MSDN Library, Internet: http://msdn.microsoft.com/en-us/library/ff648183.aspx.

[24] Oda, Wurster, van Oorschot, Somayahi, "SOMA: mutual approval for included content in web pages", October 2008 CCS '08: Proceedings of the 15th ACM conference on Computer and communications security.

[25] Coviello, Art "Open letter to RSA Customers", EMC/RSA website, Internet: http://www.rsa.com/node.aspx?id=3872, [December 27, 2011]

[26] Zetter, Kim, "RSA Agrees to Replace Security Tokens After Admitting Compromise", Threat Level, Privacy, Crime and Security Online, June 7, 2011, Internet: http://www.wired.com/threatlevel/2011/06/rsa-replaces-securid-tokens.

[27] Campbell, Al-Muhtaki, Naldurg, Sampemane, Mickunas, "Towards security and privacy for pervasive computing", ISSS'02 Porceedings of the 2002 Mext-NSF-JSPS international conference on Software security: theries and systems, Springer-Verlag Berlin, Heidelberg, pp. 1-15.

[28] Subramanian, Krishnan, "Citrix Acquires Cloud.com: An Analysis", Cloud Ave, July 12, 2011, Internet: http://www.cloudave.com/13848/citix-acquires-cloud-com-an-analysis.

[29] Belmans, Puopolo, Yellumahanti, "Network Service Providers as Cloud Providers, Survey Shows Cloud Is a Bright Option", Cisco, November 2010. Internet: http://www.cisco.com/web/about/ac79/docs/wp/sp/Service_Providers_as_Cloud_Providers_IBSG.pdf [March 28, 2012]

[30] Kessinger, Ketchum, "2011 ISACA IT Risk/Reward Barometer – North America, ISACA, http://www.isaca.org/SiteCollectionDocumnets/2011-Risk-Reward-barometer-North-America.pdf.

[31] VMware web site, VMware vCenter Server Features: Virtualization Management, Server Provisioning, Server Consolidation, Internet: http://www.vmware.com/products/vcenter-server/features.html , [October 9, 2011]

[32] VMware web site, VMware vShield: Virtualization Security for Virtual Datacenters and cloud Infrastructures, Internet: http://www.vmware.com/products/vshield/overview.html, [March 28, 2012]

[33] "ESXi configuration Guide – ESXi 4.1", Vmware, Inc., Updated 10/27/2011, Chapter 13 – Authentication and User Management, Internet: http://www.vmware.com/support/pubs/vs_pages/vsp_pubs_esxi41_i_vc41.html, [March 26, 2012]

[34] Xen Wiki. Categpru: Project, Internet: http://wiki.xen.org/wiki/Category/Project , [March 28, 2012]

[35] "What is Xen Hypervisor?", Xen.org, Internet: http://www.xen.org/files/Marketing/WhatisXen.pdf, [October 13, 2011]

[36] XEN, "How Does Xen Work?", xen.org, Version 1.0, December 2009, Internet: http://www.xen.org/files/Marketing/HowDoesXenWork.pdf, [February 25, 2012]

[37] Spector Stephen and xen.org community, "Why Xen?", Xen.org, July 30, 2010, Internet: http://www.xen.org/files/Marketing/WhyXen.pdf, [February 25, 2012]

[38] Xen Cloud Platform, Xen.org, Internet: http://www.xen.org/products/cloudxen.html, [October 13, 2011]

[39] Soundararajan, Vijayaraghavan and Govil, Kinshuk, "Challenges in Building Scalable Virtualized Datacenter Management", ACM SIGOPS Operating Systems Review, Volume 44 Issue 4, December 2010, pp 95 – 102.

[40] Eucalyptus Products page, Internet: http://www.eucalyptus.com/products/eee/functionality , [October 9, 2011]

[41] Eucalyptus Community page, Internet: http://open.eucalyptus.com/ , [November 22, 2011]

[42] "25,000 Hybrid and Private Clouds", Eucalyptus Systems, Inc., 2012, Internet: http://www.eucalyptus.com/25000clouds [February 25, 2012]

[43] Prasad Naldurg, Stefan Schwoon, Sriram Rajamani, John Lambert, "NETRA: Seeing Through Access Control", In Proceedings of the fourth ACM workshop on Formal methods in security (FMSE'06) ACM, New Your, NY, USA pp 55-66.

[44] Hansteen, Peter N. M., 2005-2012, OpenBSD as a Router and Firewall, pp. 87-88, Enternet: http://home.nuug.no/`peter/pf/en/pf-firewall.pdf

[45] Schneier Bruce, "Whitelisting vs. Blacklisting", Schneier on Security, January 28, 2011, Internet: http://www.schneier.com/blog/archives/2011/01/whitelisting_vs.html [March 29, 2012]

[46] Kundra, Vivek, U.S. Chief Information Officer, "Federal Cloud Computing Strategy", February 8, 2011, Executive Office of the President of the United States, Internet: http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf [March 28, 2012]

[47] Weber, S. G., Martucci, L. A., Ries, S., and Mühlhä user M., Towards trustworthy identity and access management for the for the future internet. In The 4th International Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS 2010) co-located with the Internet of Things 2010 Conference, November 2010. (Tokyo, Japan, Nov. 2010)

[48] Pfitzmann and Waidner, "Federated Identity-Management Protocols", Security Protocols Lecture Notes in Computer Science, 2005, Volume 3364, Springer Berlin / Heidelberg, pp. 153-174.

[49] Pfitzmann and Waidner, "Federated Identity-Management Protocols", Security Protocols Lecture Notes in Computer Science, 2005, Volume 3364, Springer Berlin / Heidelberg, pp. 153-174.

[50] Ferraiolo F. David, Kuhn D. Richard, "Role-Based Access Controls", National Institute of Standards and Technology, Technology Administration, 15th National Computer Security Conference(1992), Baltimore MD pp. 554 – 563.

[51] Belokosztolszki, Eyers, Pietzuch, Bacon, Moody "Role-Based Access Control for Publish/Subscribe Middleware Architectures", In Proceedings of the 2nd international workshop on distributed event-based systems (DEBS '03). ACM, New York, NY, USA, pp. 1-8.

[52] "Role Based Access control (RBAC) and Role Based Security", National Institute of Standards and Technology Information Technology Laboratory, Internet: http://csrc.nist.gov/groups/SNS/rbac/, [January 29, 2012]

[53] "Creating a Role that Permits Completion of a Limited Task ", ESXi and vCenter Server 5.0 Documentation, Vmware, Internet: http://pubs.vmware.com/vsphere-50/index.jsp?topic=/com.vmware.vsphere.solutions.doc_50/GUID-F3439CE6-B1FC-4165-B39B-B1877D890422.html, [February 4, 2012]

[54] "All About Amazon Simple Storage Service Reviews", Cloudingworld.com, June 9, 2011 Internet: http://cloudingworld.com/cloud-knowledge/all-about-amazon-simple-storage-service-reviews.html, [February 4, 2012]

[55] Darrow Barb, "Amazon S3, Microsoft Azure are top dogs in cloud storage", Gigacom, December 12, 2011, Internet: http://gigaom.com/cloud/amazon-s3-microsoft-azure-top-dogs-in-cloud-storage, [February 25, 2012]

[56] Grannerman Joseph, "Amazon S3 security: Exploiting misconfigurations" SearchCloudSecurity, August 2011, TechTarget. Internet: http://searchcloudsecurity.techtarget.com/tip/Amazon-S3-security-Exploiting-misconfigurations, [March 29, 2012]

[57] Vasto (Virtualization ASsesment Toolkit), Internet: http://vasto.nibblesec.org/ , [March 29, 2012]

[58] Criscione Claudio, "vmware_guest_stealer.rb", This module is part of VASTO Version 0.4 Virtualization Assessment Toolkit, Internet: http://vasto.nibblesec.org/, [February 25, 2012]

[59] CVE-2009-2267 CVE-2009-3733, The Common Vulnerabilities and Exposures project, cve.mitre.org

[60] "Security Advisories & Certifications VMSA-2009-0015", October 27, 2009, Internet: http://www.vmware.com/security/advisories/VMSA-2009-0015.html, [February 25, 2012]

[61] Oberheide Jon, Cooke Evan, Jahanian Farnam, "Empirical Exploitation of Live Virtual Machine Migration", in BlackHat DC 2008, Washington, DC, 2008.

[62] Thomas Ristenpart, Eran Tromer, hovav Shacham, Stefan Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds", ACM Conference on Computer and Communications Security, November 2009.

[63] Posey, Brien M, "Networking Basics: Part 15 – Universal Groups & Group Nesting" WindowsNetworking.com, May 14, 2008 Internet: http://www.windowsnetworking.com/articles_tutorials/Networking-Basics-Part15.html , [March 3, 2012]

[64] vsphere-esxi-vcenter-server-50-networking-guide.pdf, 2009–2011 VMware, Inc Internet: http://www.vmware.com/support/pubs, [March 29, 2012]

[65] Openfiler web site, Internet: www.openfiler.com, [March 11, 2012]

[66] C. Finseth, "An Access Control Protocol, Sometimes Called TACACS", RFC 1492 University of Minnesota, July 1992

[67] Microsoft windows update services home, 2005, Microsoft Inc. Internet: http://www.microsoft.com/wsus.

[68] VMware, VMware vcenter update manager, Internet: http://www.vmware.com/products/update-manger, [March 29, 2012]

[69] Marcus J. Ranum, Thinking About Firewalls, In Proceedings of the 2nd International Conference on systems and Network Security and Management (SANS-11), April 1993.

[70] Eucalyptus Community, "Eucalyptus Administrator's Guide (2.0)", Internet: http://open.eucalyptus.com/book/export/html/4263, [January 1, 2012]

[71] "Juniper Networks Technical Documentation", Internet: http://www.juniper.net/techpubs/en_US/junos10.4/topics/concept/zone-and-interface-overview.html, [February 26, 2012]

[72] "Likewise Open Installation and Administration Guide", Internet: http://www.beyondtrust.com/Technical-Support/Downloads/files/pbiso/Manuals/likewise-open-60-guide.html. Last updated: May 10, 2011. [March 29, 2012]

[73] VMware Knowledge Base website, “Enabling logging for Likewise agents on ESX/ESXi” Internet: http://kb.vmware.com. [Feb 27, 2012]

[74] “Microsoft TechNet: Server 2003: Security Identifiers Technical Reference”, Updated: -- March 28, 2003. Internet: http://technet.microsoft.com/en-us/library/cc782090.aspx, [March 29, 2012]